UTN.BA UNIVERSIDAD TECNOLÓGICA NACIONAL FACULTAD REGIONAL BUENOS AIRES | Centro de e-Learning Secretaría de Cultura y Extensión Universitaria

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Experto Universitario en Ethical Hacking

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Módulo 2:

Administración de Servidores (Windows o Linux)

Unidad 2:

Roles y funciones de un servidor

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Presentación

En esta segunda Unidad del módulo, conocerán los roles más importantes que se pueden encontrar en los servidores.

Aprenderán sobre las funciones que ofrecen a nivel servicios.

Y a la par, los servicios asociados para poder brindar una conectividad y operatividad segura.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Objetivos

Que los participantes logren…

- Conocer sobre el mundo de los servidores informáticos, existentes en toda infraestructura informática de mediana y alta gama.

- Conocer las herramientas esenciales y las buenas prácticas necesarias para obtener el máximo nivel de seguridad en una red de servidores de arquitectura Microsoft Windows Server o Linux Server, protegiéndola de potenciales amenazas.

- Comprender los conceptos básicos referentes a la implementación, configuración, mantenimiento y soporte de servidores de infraestructura en tecnologías Windows o Linux.

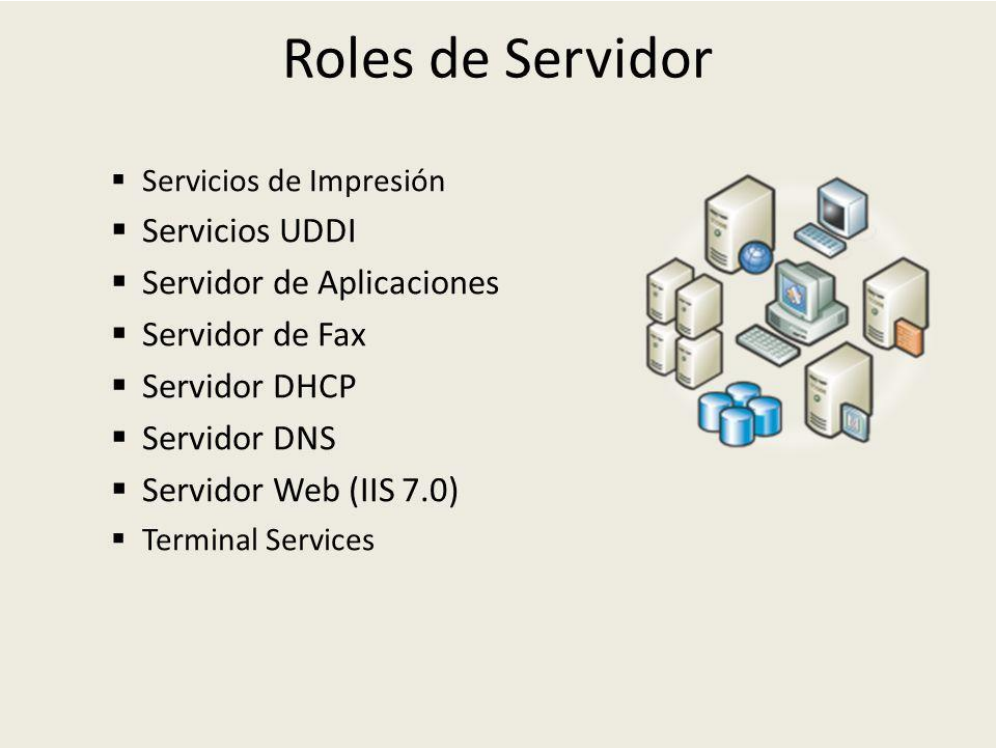
Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Bloques temáticos

1. Tipos de Roles.
2. Funciones de un servidor.
3. Servicios asociados a un servidor.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Tipos de Roles



Los más utilizados:

Servidor dedicado: toda su potencia está dedicada a resolver las solicitudes de los clientes.

Es un servidor comprado o arrendado que se utiliza para prestar servicios dedicados exclusivamente a un cliente, generalmente relacionados con el alojamiento web y otros servicios en red.

A diferencia de lo que ocurre con el alojamiento compartido, en donde los recursos de la máquina son compartidos entre un número indeterminado de clientes, en el caso de los servidores dedicados generalmente es un solo cliente el que dispone de todos los recursos para los fines por los cuales haya contratado el servicio.

Los Servidores Dedicados son máquinas físicas de uso exclusivo para un cliente.

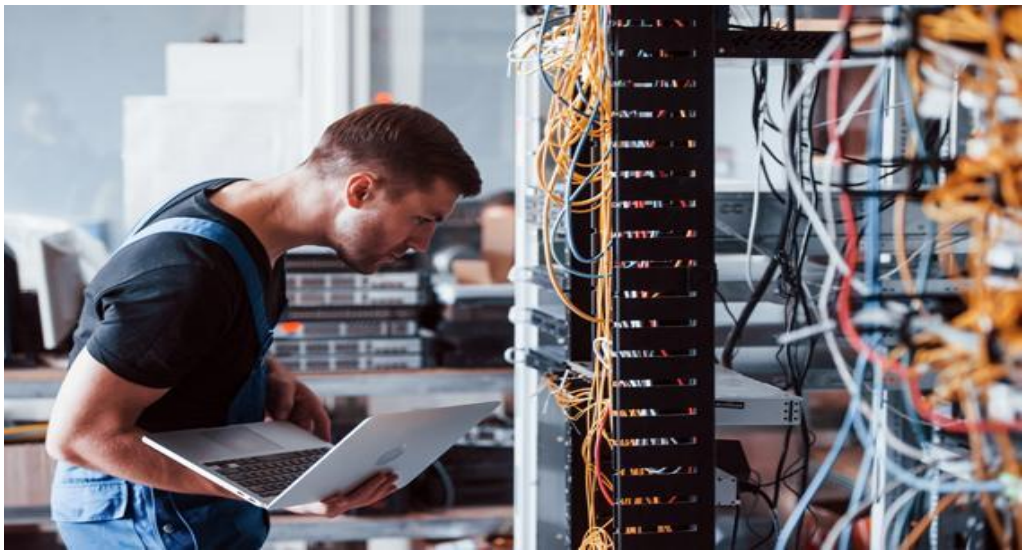
Al contratar un Servidor Dedicado se obtiene todos los recursos de manera exclusiva, como el espacio, ancho de banda, transferencias, etc.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Con este tipo de alojamiento web se puede decidir si se quiere un Servidor administrado o autoadministrado.

En caso de contratar un servidor autoadministrado se puede dedicar totalmente al desarrollo y crecimiento del sitio web y se podrá gestionar los recursos, accesos, firewall, etc.

¿Quién se encarga del Mantenimiento?



Generalmente, el cuidado físico de la máquina y de la conectividad a Internet está generalmente a cargo de la empresa que provee el servidor.

Un servidor dedicado regularmente se encuentra localizado en un centro de datos, que es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico.

Ahora bien, hablemos también de algunas peculiaridades de estos servidores y que un servidor dedicado puede ser utilizado como una forma avanzada de alojamiento web cuando un cliente o empresa tiene requerimientos especiales de rendimiento, configuración o seguridad.

En estos casos es común que una empresa arriende un servidor dedicado para autoabastecerse de los servicios que necesita disponiendo de todos los recursos de la máquina.

Servidor no dedicado: son aquellos que comparten su potencia entre las respuestas a los clientes y posibles solicitudes de un usuario local.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

¿Qué es un Servidor Dedicado Windows?

Este tipo de servidor web, es muy efectivo principalmente en dos puntos preponderantes como son el control y la confiabilidad.

Esto se debe a que los administradores ponen mucha más atención y vigilancia sobre un servicio dedicado que a uno compartido, es por ello que el nivel de seguridad aumenta.

Hay que comprender que existen desventajas, la principal de ellas es el alto costo de contratación que conlleva un servicio de este tipo, aparte de la gestión relacionada con la seguridad.

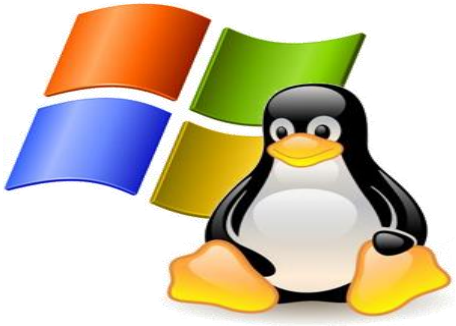
¿Qué es el Servidor Dedicado Linux?

Es una plataforma que resulta ser mucho más económica y accesible, solo que su negatividad radica en que es muy complicado de mantener, mucho más para aquellos que no lo han tratado.

Ambas plataformas se presentan con altos niveles de confiabilidad, dado que ya llevan una trayectoria de varios años que son avalados por sus logros.

Además, cada uno cuenta con equipos de profesionales y técnicos que se encuentran en un constante proceso de trabajo y actualización de sus componentes para estar al día con los últimos avances tecnológicos.

¿Cuál elegir?



La recomendación, es no elegir por el sistema operativo, sino por la necesidad y la demanda que uno tiene que tener en cuenta, no hay nada garantizado que un **SO** es mejor que el otro en un 100%, lo bueno de uno, quizás en el otro es mejor o peor, por eso todo dependerá de lo que uno realmente necesite.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Funciones de un servidor

Todos los servidores comparten la función común de proporcionar el acceso a los archivos y servicios. Una de las funciones más habituales de los servidores informáticos es prestar servicios de red.

Entre las funciones principales de los servidores informáticos tenemos:

Acceso a los datos desde la casa o desde la oficina

Si instala un servidor en su empresa, puede proporcionar acceso a documentos, hojas de cálculo, mensajes de correo electrónico y otros datos necesarios para los trabajadores que no se encuentran físicamente en la empresa.

De ese modo, los “teletrabajadores”, los empleados que viajan y los que se encuentran en otras oficinas, tienen la posibilidad de compartir datos.

Incluso podrán acceder al equipo personal con el que trabajan en la oficina.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

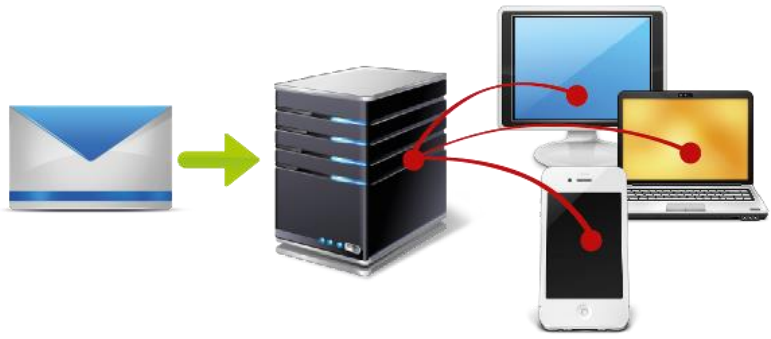
Alojamiento de una intranet

Una **intranet** es un sitio web interno de una compañía, universidad, empresa, escuela, etc., que a través del cual se puede proporcionar información exclusivamente para los empleados, alumnos.

Los mismos tienen la posibilidad de utilizar el sitio para publicar información y colaborar en la elaboración de documentos.

También es posible utilizar el sitio para publicar anuncios, eventos, calendarios y vínculos a recursos importantes de estas instituciones.

Alojamiento del correo electrónico de la empresa, universidad, escuelas, entes gubernamentales



Se puede configurar un servidor para administrar el correo.

Eso significa que los buzones de los empleados y alumnos residirán en el servidor electrónico de la empresa o universidad, no en el de un proveedor de servicios de internet.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Acceso a datos desde un dispositivo móvil

Los servidores también pueden permitir el acceso a los datos desde teléfonos móviles u otros dispositivos portátiles que se conectan a internet.

Los empleados de una empresa que utilicen dispositivos móviles pueden obtener acceso y consultar el correo electrónico o actualizar contactos y calendarios a cualquier hora del día, como si se encontraran delante de su equipo de sobremesa.

Uso de programas en empresas, universidades, bibliotecas, centros de investigación, que dependen de bases de datos

Si incorpora un servidor a la empresa o universidad, los cuales puede utilizar programas especiales diseñados para funcionar con una base de datos.

Si se instala la base de datos de clientes del programa de gestión de clientes (**CRM**), todos los empleados de la organización o estudiantes de la universidad que utilicen esos datos pueden obtener acceso y trabajar con ellos.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Servicios asociados a un servidor

Vamos a conocer algunos servicios muy conocidos cuando se habla de servidores y seguridad.

DHCP

El Protocolo de configuración dinámica de host **(DHCP, Dynamic Host Configuration Protocol)** es un estándar diseñado para reducir la complejidad de la administración de configuraciones de direcciones mediante la utilización de un equipo para administrar de forma centralizada las direcciones IP y detalles de configuración de la red.

Incluye el protocolo **MADCAP (Multicast Address Dynamic Client Assignment Protocol)**, que se utiliza para realizar la asignación de direcciones de multidifusión.

Los clientes registrados a los que se asigna dinámicamente una dirección IP mediante **MADCAP** pueden participar de forma eficaz en el proceso de transmisión por secuencias de datos como, por ejemplo, en transmisiones en tiempo real de vídeo o sonido a través de la red.

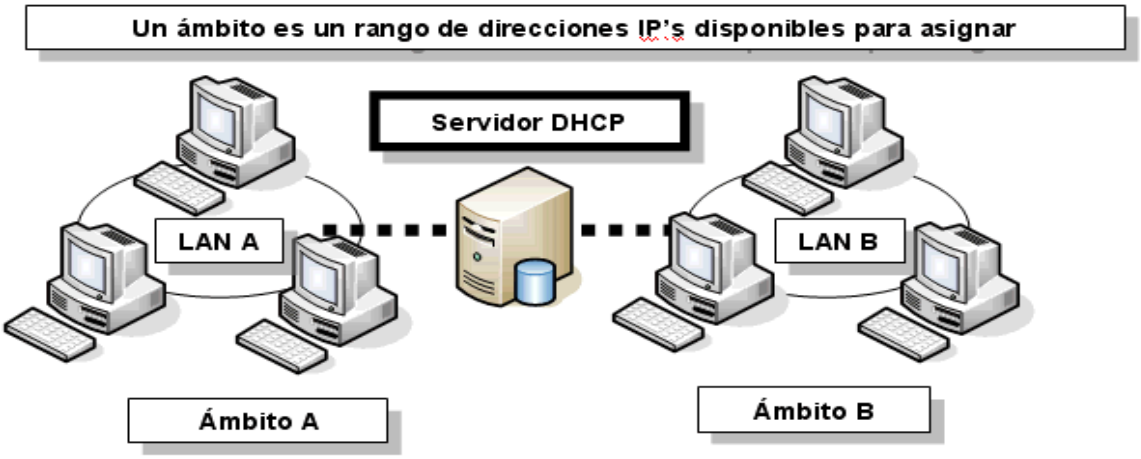
Todos los equipos y otros dispositivos de la red **TCP/IP** deben tener una dirección **IP** para que la red funcione correctamente.

Las direcciones **IP** se pueden configurar manualmente en cada equipo o puede implementar un servidor **DHCP** que asigne automáticamente concesiones de direcciones **IP** a todos los clientes **DHCP** de la red.

Dado que la mayoría de los sistemas operativos cliente buscan una concesión de dirección **IP** de forma predeterminada, no es necesario establecer ninguna configuración en el equipo cliente para implementar una red habilitada para **DHCP**; el primer paso es implementar un servidor **DHCP**.

No obstante, para que el servidor **DHCP** pueda proporcionar concesiones de direcciones de **IP** a los clientes, se debe definir un intervalo de direcciones **IP** en el servidor **DHCP**.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning



Este intervalo, llamado ámbito, define una sola subred física en la red en la que se proporcionan los servicios **DHCP**.

Por lo tanto, si tiene dos subredes, por ejemplo, el servidor **DHCP** debe estar conectado a cada subred y debe definir un ámbito para cada subred.

Además, los ámbitos son el método principal para que el servidor administre la distribución y la asignación de direcciones **IP** además de cualquier parámetro de configuración relacionado para los clientes de la red.

DNS

El sistema de nombres de dominio (**DNS**) es un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios.

Las redes **TCP/IP**, como Internet, usan **DNS** para buscar equipos y servicios mediante nombres descriptivos.

Para que el uso de los recursos de red sea más fácil, los sistemas de nombres como **DNS** proporcionan un método para asignar el nombre descriptivo de un equipo o servicio a otros datos asociados a dicho nombre, como una dirección **IP**.

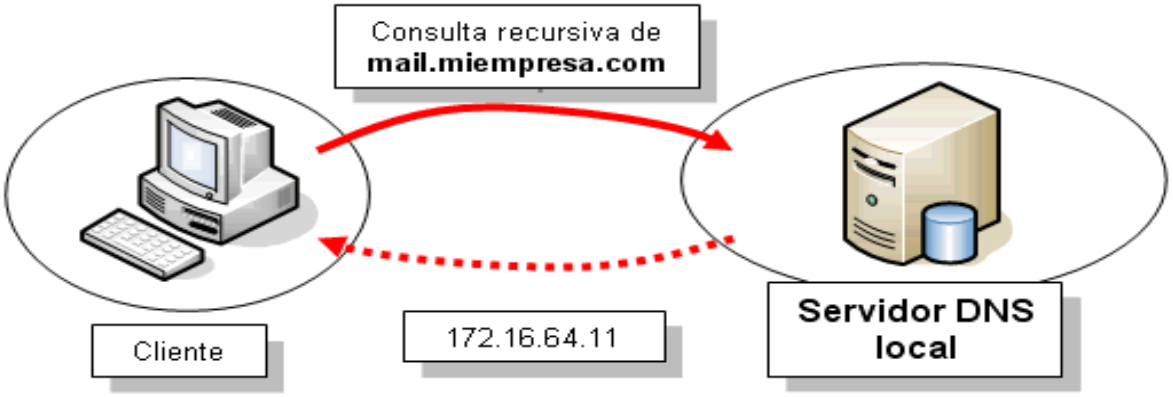
Un nombre descriptivo es más fácil de aprender y recordar que las direcciones numéricas que los equipos usan para comunicarse a través de una red.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

La mayoría de la gente prefiere usar un nombre descriptivo (por ejemplo, mailar.telefon.com) para buscar un servidor de correo electrónico o servidor web en una red en lugar de una dirección IP, como 157.60.0.1.

Cuando un usuario escribe un nombre **DNS** descriptivo en una aplicación, los servicios **DNS** convierten el nombre en su dirección numérica.

Supongamos que buscamos una dirección web, al realizar la consulta, nos devolverá su ubicación a través de una dirección **IP**, que si la misma se encuentra enrutada, podremos encontrarla.



Que tener en cuenta en un servidor DNS con respecto a la seguridad

A continuación, para aclarar lo referente al Sistema de Nombres de Dominio (**DNS**), una introducción sobre la seguridad de los Servidores, posibles amenazas y distintas alternativas de protección, según la configuración de seguridad que se puede realizar.

Información de seguridad para DNS:

El Sistema de nombres de dominio (**DNS**) se diseñó originalmente como un protocolo abierto. Por lo tanto, resulta vulnerable ante los atacantes.

El **DNS** de Windows Server 2008 por ejemplo, ayuda a mejorar la capacidad de impedir ataques en la infraestructura **DNS** mediante la adición de características de seguridad.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Antes de considerar qué características de seguridad se deben usar, hay tener en cuenta las amenazas más habituales contra la seguridad **DNS** y el nivel de seguridad **DNS** de la organización.

Amenazas de seguridad DNS:

A continuación, se indican las formas habituales en las que la infraestructura DNS puede verse amenazada por los atacantes:

- **Representación**: Proceso mediante el que un atacante obtiene los datos de la zona **DNS** a fin de conseguir nombres de dominio **DNS**, nombres de equipo y direcciones **IP** de recursos de red confidenciales.

  El atacante suele iniciar un ataque con estos datos **DNS** para hacer un diagrama o "representación" de una red. El dominio **DNS** y los nombres de equipo normalmente indican la función o la ubicación de un dominio o de un equipo para ayudar a los usuarios a recordar e identificar dominios y equipos de una manera más fácil. El atacante aprovecha el mismo principio de **DNS** para conocer la función o la ubicación de dominios y equipos de la red.

- **Ataque por denegación de servicio**: Intento de un atacante de denegar la disponibilidad de los servicios de red al congestionar uno o varios servidores **DNS** de la red con consultas recursivas. Cuando un servidor **DNS** se congestiona con consultas, su uso de **CPU** termina alcanzando el nivel máximo y el servicio Servidor **DNS** deja de estar disponible. Sin un servidor **DNS** completamente operativo en la red, los servicios de ésta que usan **DNS** no están disponibles para los usuarios de la red.

- **Modificación de datos**: Intento de un atacante (que realizó una representación de una red con **DNS**) de usar direcciones **IP** válidas en paquetes **IP** que ha creado él mismo. De este modo, parece que estos paquetes proceden de una dirección **IP** válida de la red. Esto se denomina habitualmente "**Suplantación de IP**".

  Con una dirección **IP** válida (una dirección **IP** dentro del intervalo de direcciones **IP** de una subred), el atacante puede obtener acceso a la red y destruir datos, o bien realizar otros ataques.

- **Redirección**: El atacante busca redirigir las consultas de los nombres **DNS** a los servidores que se encuentran bajo su control. Los métodos de redirección intentan contaminar la caché **DNS** de un servidor **DNS** con datos **DNS** incorrectos que puedan dirigir las futuras consultas a servidores que controla el atacante.

  Por ejemplo, si originalmente se realizó una consulta para widgets.tailspintoys.com y una respuesta de referencia proporciona una registro para un nombre que se encuentra fuera del dominio tailspintoys.com, como usuario-malintencionado.com, el servidor **DNS** usa

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

los datos en caché de usuario-malintencionado.com para resolver una consulta relativa a dicho nombre.

Los atacantes pueden lograr la redirección siempre que tengan acceso de escritura a datos **DNS**, por ejemplo, cuando las actualizaciones dinámicas no son seguras.

Tipos de registros:

Un **DNS** es una base de datos distribuida que contiene registros que se conocen como **RR** (Registros de Recursos), relacionados con nombres de dominio. La siguiente información sólo es útil para las personas responsables de la administración de un dominio, dado que el funcionamiento de los servidores de nombre de dominio es completamente transparente para los usuarios.

Ya que el sistema de memoria caché permite que el sistema **DNS** sea distribuido, los registros para cada dominio tienen una duración de vida que se conoce como **TTL** (Tiempo de vida).

Esto permite que los servidores intermediarios conozcan la fecha de caducidad de la información y por lo tanto que sepan si es necesario verificarla o no.

Por lo general, un registro de **DNS** contiene la siguiente información:

Nombre de dominio (FQDN)	TTL	Tipo	Clase	RData
es.kioskea.net	3600	A	IN	163.5.255.85

Nombre de dominio: El nombre de dominio debe ser un nombre FQDN, es decir, debe terminar con un punto.

En caso de que falte el punto, el nombre de dominio es relativo, es decir, el nombre de dominio principal incluirá un sufijo en el dominio introducido;

Tipo: Un valor sobre 16 bits que define el tipo de recurso descrito por el registro. El tipo de recurso puede ser uno de los siguientes:

A: este es un tipo de base que hace coincidir el nombre canónico con la dirección **IP**. Además, pueden existir varios registros A relacionados con diferentes equipos de la red (servidores).

CNAME (Nombre Canónico): Permite definir un alias para el nombre canónico. Es particularmente útil para suministrar nombres alternativos relacionados con diferentes servicios en el mismo equipo.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

HINFO: éste es un campo solamente descriptivo que permite la descripción en particular del hardware del ordenador (**CPU**) y del sistema operativo (**OS**). Generalmente se recomienda no completarlo para evitar suministrar información que pueda ser útil a piratas informáticos.

MX (Mail Exchange): es el servidor de correo electrónico. Cuando un usuario envía un correo electrónico a una dirección (user@domain), el servidor de correo saliente interroga al servidor de nombre de dominio con autoridad sobre el dominio para obtener el registro **MX**.

Pueden existir varios registros **MX** por dominio, para así suministrar una repetición en caso de fallas en el servidor principal de correo electrónico.

De este modo, el registro **MX** permite definir una prioridad con un valor entre 0 y 65,535.

NS: es el servidor de nombres de dominio con autoridad sobre el dominio.

PTR: es un puntero hacia otra parte del espacio de nombres del dominio.

SOA (Start Of Authority (Inicio de autoridad)): el campo SOA permite la descripción del servidor de nombre de dominio con autoridad en la zona, así como la dirección de correo electrónico del contacto técnico (en donde el carácter "@" es reemplazado por un punto).

Clase: la clase puede ser IN (relacionada a protocolos de Internet, y por lo tanto, éste es el sistema que utilizaremos en nuestro caso), o CH (para el sistema caótico).

RDATA: estos son los datos relacionados con el registro. Aquí se encuentra la información esperada según el tipo de registro:

- A: la dirección IP de 32 bits:
- CNAME: el nombre de dominio;
- MX: la prioridad de 16 bits, seguida del nombre del ordenador;
- NS: el nombre del ordenador; PTR: el nombre de dominio
- PTR: el nombre de dominio;
- SOA: varios campos.

Por último cuando hablamos de dominios, nos encontramos con los de nivel superior:

Existen dos categorías de TLD (Dominios de Nivel Superior):

Los dominios que se conocen como "genéricos", llamados **gTLD (TLD genérico)**.

Los **gTLD** son nombres de dominio de nivel superior genéricos que ofrecen una clasificación de acuerdo con el sector de la actividad.

Entonces cada **gTLD** tiene sus propias reglas de acceso:

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

gTLD historial:

- **.arpa** relacionado con equipos pertenecientes a la red original;
- **.com** inicialmente relacionado con empresas con fines comerciales. Sin embargo, este **TLD** se convirtió en el "**TLD** predeterminado" y hasta personas reales pueden adquirir dominios con esta extensión.
- **.edu** relacionado con las organizaciones educativas;
- **.gov** relacionado con las organizaciones gubernamentales;
- **.int** relacionado con las organizaciones internacionales;
- **.mil** relacionado con las organizaciones militares;
- **.net** inicialmente relacionado con las organizaciones que administran redes. Con el transcurso de los años este **TLD** se ha convertido en un **TLD** común, y hasta personas reales pueden adquirir dominios con esta extensión.
- **.org** está normalmente relacionado con organizaciones sin fines de lucro.
- A medida que pasan los años salen nuevos **gTLD**:
- **.aero** relacionado con la industria aeronáutica;
- **.biz** (negocios) relacionado con empresas comerciales;
- **.museum** relacionada con los museos;
- **.name** relacionada con el nombre de personas reales o imaginarias;
- **.info** relacionado con organizaciones que manejan información;
- **.coop** relacionado con cooperativas;
- **.pro** relacionado con profesiones liberales.

Los dominios que se conocen como "nacionales", se llaman **ccTLD (código de país TLD)**.

El **ccTLD** está relacionado con los diferentes países y sus nombres se refieren a las abreviaturas del nombre del país definidas en la norma **ISO 3166.**

A continuación, algunos ejemplos de la lista de **ccTLD.**

CÓDIGO: **AR** (Argentina), **CO** (Colombia), **ES** (España), **HK** (Hong Kong), **NZ** (Nueva Zelanda), **UK** (Reino Unido), **ZA** (Sudáfrica).

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

WINS

Es una aplicación de **Microsoft** que resuelve los nombres **NetBIOS**, los nombres que utilizamos generalmente para referirnos a los ordenadores.

El servicio **WINS** consta de dos componentes principales: el servidor **WINS** y los Clientes **WINS**.

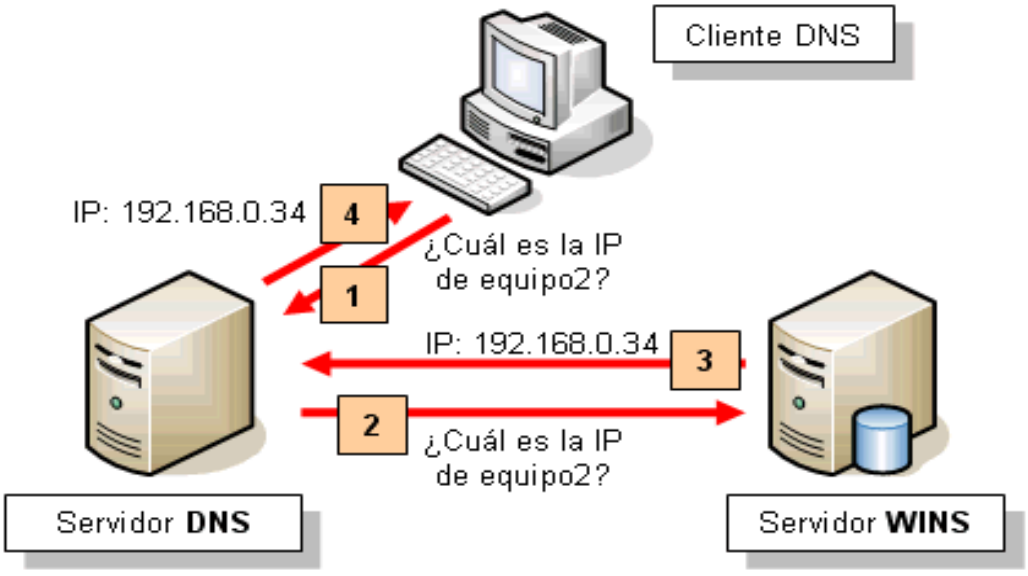
El servidor **WINS** controla las solicitudes de registro de nombres de los clientes **WINS** y registra sus nombres y sus direcciones **IP**; asimismo, responde a las consultas de nombres **NetBIOS** que emiten los clientes y devuelve la dirección **IP** del nombre consultado si se encuentra en la base de datos del servidor.

Ventajas

Administración centralizada de la base de datos para asignar direcciones a los nombres, con lo que se reduce la necesidad de administrar archivos **Lmhost.**

Base de datos dinámica para asignar direcciones a los nombres que permite el registro y la resolución de nombres de equipo.

Compatibilidad con clientes **DNS**, al permitirles encontrar recursos **NetBIOS** cuando está implementada la Integración de la búsqueda **WINS**.



Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Balanceo de Carga

Es la técnica de distribuir equitativamente el peso del cómputo entre varios dispositivos.

Su objetivo es conseguir que todos los elementos que llevan a cabo la misma tarea, estén igualmente cargados con el fin de aumentar la potencia de cálculo, la disponibilidad y la calidad del servicio.

Un sistema de balanceo de carga no implica necesariamente una tolerancia a fallos. El elemento que ha fallado perderá sus procesos y deberán ser creados de nuevo en el resto de los servidores que soportan el balanceo.

Existen tres clases de algoritmos de balanceo:

- **Balanceo centralizado:** Un nodo ejecuta el algoritmo y mantiene el estado global del sistema.
- **Balanceo semi-distribuido:** Los procesadores son clasificados y divididos por regiones, cada región tiene un algoritmo centralizado local, mientras otro algoritmo balancea la carga entre las regiones.

  El balanceo puede ser iniciado por envío o recibimiento. Si es balanceo iniciado por envío, un procesador con mucha carga envía trabajo a otros.

  Si es balanceo iniciado por recibimiento, un procesador con poca carga solicita trabajo de otros.

  Si la carga por procesador es baja o mediana, es mejor el balanceo iniciado por envío. Si la carga es alta se debe usar balanceo iniciado por recibimiento.

  De lo contrario, en ambos casos, se puede producir una fuerte migración innecesaria de tareas.
- **Balanceo completamente distribuido**: Cada procesador mantiene su propia visión del sistema intercambiando información con sus vecinos y así poder realizar cambios locales.

Todos los elementos de una red fuertemente utilizados admiten de algún modo que su carga sea balanceada con otros dispositivos semejantes.

Entre los elementos de una red más susceptibles de ser balanceados se encuentran servidores, servicios Web, líneas de comunicaciones y routers/switches/firewalls.

Balanceo de carga entre Firewalls

Se utilizan para dar continuidad al servicio de acceso a Internet de la compañía.

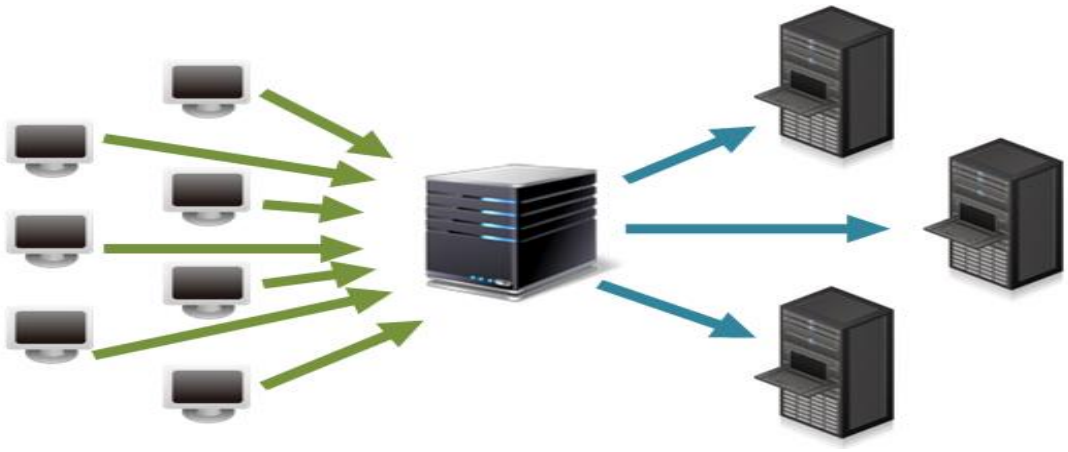
La tabla de conexiones es compartida entre todos los cortafuegos que atienden selectivamente las conexiones.

Balanceo de carga entre líneas de comunicaciones.

Esta técnica consiste en agrupar varias líneas de comunicaciones, por ejemplo ADSL, para conseguir una única línea de mayor capacidad.

Todas las líneas pueden utilizarse a la vez, la carga es compartida y las conexiones desde el exterior son balanceadas por el dispositivo de balanceo de carga.

Balanceo de Carga entre Servidores



La Tecnología de Balance de Carga entre servidores intenta eliminar los puntos de falla en comunicación y transferencia de archivos.

Balanceando la carga en los servidores, ya que el mismo posee múltiples caminos para acceder a los sistemas.

Varios métodos conocidos:

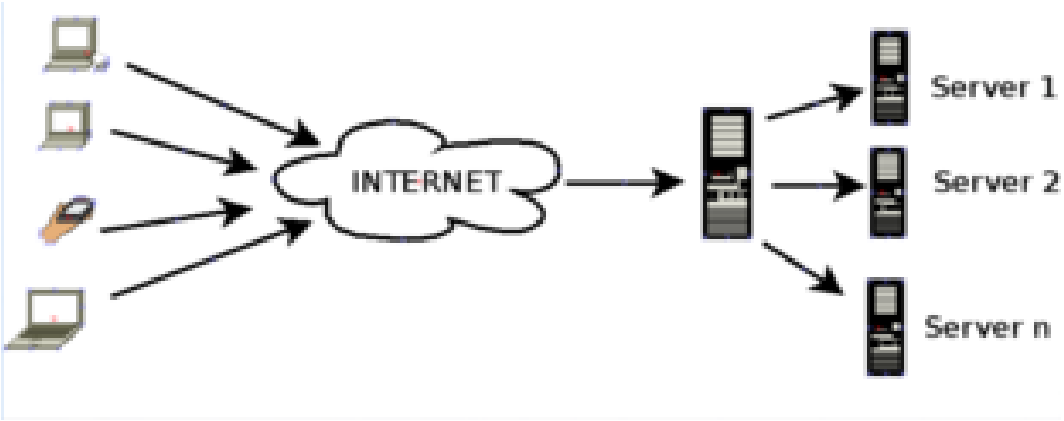
- **Round Robin**
- **Passive Polling**
- **Nodo de balanceo**
- **Enrutamiento directo**

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

- **Encapsulado IP**
- **Nat**

Hablemos de los 3 primeros:

DNS Round Robin es una técnica de balanceo de carga o tolerancia a fallos de aprovisionamiento múltiple y redundante para servidores de servicios IP, por ejemplo, servidores web o servidores FTP, que utiliza la gestión de nombres de dominio (DNS del sistema) para hacer frente a las peticiones de los equipos cliente según un modelo estadístico pertinente.



Es relativamente sencillo de implementar; consiste en responder a las solicitudes **DNS** con una lista de direcciones **IP** de varios servidores que ofrezcan servicios idénticos, en vez de responder con una sola dirección.

El orden en que se devuelven las direcciones **IP** de la lista es la base del término **Round-Robin**.

Con cada respuesta de **DNS**, es permutada la secuencia de direcciones **IP** en la lista.

Por lo general, los clientes **IP** básicos intentan conectar con la primera dirección que ha sido devuelta en la consulta **DNS**, a fin de que los clientes al realizar diferentes intentos, puedan recibir el servicio de diferentes proveedores, con lo que la **distribución de la carga global** se distribuya entre los servidores.

Las peticiones de los clientes son distribuidas equitativamente entre todos los servidores existentes.

Sin embargo, este método cíclico no tiene en cuenta las condiciones y carga de cada servidor.

Esto puede implicar que haya servidores que reciben peticiones de carga mucho mayor, mientras hay servidores que apenas se encuentran utilizando recursos.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Passive Polling calcula el tiempo de respuesta de los servidores y tiene una referencia de su estado. En este método no se tiene en cuenta la variedad de servidores empleados.

Además, sólo descubre que los servidores tienen un problema después de que se produzcan retrasos o, en el peor de los casos, cuando los servidores están completamente caídos.

Nodo de balanceo Los clientes que se conecten al servidor acceden a través de un único punto de entrada, un nodo que será el balanceador de carga, el cual, de forma transparente dirigirá el tráfico a cualquiera de los nodos disponibles.

Un nodo balanceador de carga, ofrece numerosas ventajas:

– Puede actuar como *firewall*.

– Puede asignar cargas de trabajo asimétricas, de manera que algunos nodos reciban más o menos peticiones en función de sus capacidades.

– Tiene tolerancia a fallos de los nodos servidores.

– Se puede realizar monitorización del estado en que se encuentran los nodos servidores.

– Se puede considerar una infraestructura clúster.

Otros métodos de balanceo:

– Balanceo por enrutamiento directo

– Balanceo mediante encapsulado IP

– Balanceo NAT

Clúster y su función en una red

Un clúster es un conjunto de equipos de cómputo que se comportan como una supercomputadora única.

Son utilizados principalmente para la solución de problemas de alto costo computacional referentes a las ciencias, las ingenierías y el comercio.

Este tipo de sistemas se basa en la unión de varios servidores que trabajan como si de uno sólo se tratase.

¿Qué debemos tener en cuenta para clasificar un cluster?

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Los clúster de computadoras se pueden clasificar en la combinación de las siguientes características generales:

- **Alto rendimiento**
- **Alta disponibilidad**
- **Balanceo de carga**
- **Escalabilidad**
- **Componentes de un clúster**
- **Nodos**
- **Almacenamiento**
- **Sistemas operativos**
- **Conexiones de red**
- **Middleware**
- **Protocolos de comunicación y servicios**
- **Aplicaciones**
- **Ambientes de programación paralela**

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Ejercicio Número 1 Unidad 2

A- ¿Si tuviéramos a nuestra disposición un servidor DNS, cuales piensan que serían los puntos a tener en cuenta en su creación respecto a la seguridad?

B- ¿En nuestro entorno de trabajo, en caso de disponer un servidor de DNS o DHCP, que sabemos de ellos?

C- De los distintos balanceadores de carga que vimos, ¿cuál sería el más conveniente para nuestra empresa y porque? (o sea justificar la respuesta.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la "X" el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy IMPORTANTE que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Bibliografía utilizada y sugerida

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learni the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU

Links complementarios

www.f5.com: Excelente artículo sobre administración de VMs y Servidores

https://technet.microsoft.com/es-es/library/cc764246.aspx

Sitio para bajar ISO de S.O.: ***https://tb.rg-adguard.net/index.php***

En caso de que los links que se exponen no funcionen, por favor avisar al instructor (es normal que un sitio pueda cambiar su URL, dominio o variables, lo cual como la unidad se prepara a principio de año podría suceder que se haya modificado).