Práctica 4

Capa de Aplicación - MAIL

Grupo z
Integrantes: Herrera Francisco, Domé Luis y Gagliardi Pablo.

7. (Ejercicio de promoción) Integrador HTTP, DNS y MAIL

Suponga que se registró bajo su propiedad el dominio redes2022.com.ar y dispone de 4 servidores:

- Un servidor DNS instalado configurado como primario de la zona redes2022.com.ar. (hostname: ns1 ip: 203.0.113.65).

- Un servidor DNS instalado configurado como secundario de la zona redes2022.com.ar. (hostname: ns2 / ip: 203.0.113.66).

- Un servidor de correo electrónico (hostname: mail / ip: 203.0.113.111). Permitirá a los usuarios envíar y recibir correos a cualquier dominio de Internet.

- Un servidor WEB para el acceso a un webmail (hostname: correo / ip: 203.0.113.8). Permitirá a los usuarios gestionar vía web sus correos electrónicos a través de la URL https://mail.redes2022.com.ar

a. ¿Qué información debería informar al momento del registro para hacer visible a Internet el dominio registrado?

Los datos necesarios para registrar un dominio son:

- **Registrador oficial de dominios:** Empresa registradora oficial inscrita en ICANN la cual se encarga de preservar los datos de los registros. (nic.ar en nuestro caso, administra el Registro de nombres de dominio y asegura el funcionamiento del DNS para el ccTLD .ar).
- **Propietario del dominio:** Persona o entidad que figura como propietario y legítimo dueño por el periodo de registro.

- **Contacto administrativo:** Persona o entidad designada por el propietario que figura como administrador de los datos del dominio en favor del propietario.

- **Contacto técnico:** Persona o entidad que se encarga del mantenimiento de los números DNS del dominio para su correcto funcionamiento y enlace en la red.

- **Contacto de facturación:** Persona o entidad que se encargará de realizar el pago por las correspondientes renovaciones del dominio.

- **DNS (Servidor de Nombres de Dominio)**: Estos números (mínimo 2) figuran en el registro de los dominios y muestran las direcciones IPs de los servidores que se harán cargo de las peticiones al dominio y de redirigir las mismas a donde proceda

según la naturaleza de cada petición.(hostname: ns1 ip: 203.0.113.65).(hostname: ns2 / ip: 203.0.113.66).

b. ¿Qué registros sería necesario configurar en el servidor de nombres? Indique toda la información necesaria del archivo de zona. Puede utilizar la siguiente tabla de referencia (evalúe la necesidad de usar cada caso los siguientes campos): Nombre del registro, Tipo de registro, Prioridad, TTL, Valor del registro.

Breve explicación de los campos:

TTL es el tiempo de vida del registro de recurso; determina cuándo un recurso debería ser eliminado de una caché.

El significado de Nombre y Valor depende del campo Tipo:

• Si Tipo=**A**, entonces Nombre es un nombre de host y Valor es la dirección IP correspondiente a dicho nombre. No tienen campo de prioridad.

• Si Tipo=**NS**, entonces Nombre es un dominio y Valor es el nombre de host de un servidor DNS autoritativo que sabe cómo obtener las direcciones IP de los hosts del dominio. Este registro se utiliza para encaminar las consultas DNS a lo largo de la cadena de consultas.

• Si Tipo=**CNAME**, entonces Valor es un nombre de host canónico correspondiente al alias especificado por Nombre. Este registro puede proporcionar a los hosts que hacen consultas el nombre canónico correspondiente a un nombre de host.

• Si Tipo=**MX**, entonces Valor es el nombre canónico de un servidor de correo que tiene un alias dado por Nombre. Los registros MX permiten a los nombres de host de los servidores de correo tener alias simples. Observe que utilizando el registro MX, una empresa puede tener el mismo alias para su servidor de correo y para uno de sus otros servidores (como por ejemplo, el servidor web). Para obtener el nombre canónico del servidor de correo, un cliente DNS consultaría un registro MX y para conocer el nombre canónico del otro servidor, consultaría el registro CNAME.

• Si Tipo=**SOA**, entonces es un registro de "inicio de autoridad" de DNS y almacena información importante sobre un dominio o una zona, como la dirección de correo electrónico del administrador, cuándo se actualizó el dominio por última vez y cuánto tiempo debe esperar el servidor entre actualizaciones. Todas las zonas DNS necesitan un registro SOA para ajustarse a las normas de IETF. Los registros SOA también son importantes para las transferencias de zona.

```
$ORIGIN redes2022.com.ar. 86400; el comienzo de este archivo de zona en el espacio de nombres
$TTL 3600                     ; tiempo de vencimiento (en segundos) por default en los RR sin
                              ; su propio TTL

@       SOA     dns1.redes2022.com.ar. admin.redes2022.com.ar.(
                2001062501 ; número de serie
                21600      ; refresh luego de 6 horas
                3600       ; reintentar luego de 1 hora
                604800     ; expira luego de 1 semana
                86400 )    ; TTL mínimo de 1 dia
;
;
        NS      dns1.redes2022.com.ar.
        NS      dns2.redes2022.com.ar.
dns1    A       203.0.113.65
```

```
dns2    A       203.0.113.66
;
;
@       MX      10      mail.redes2022.com.ar.
mail    A       203.0.113.111
correo  MX      20      mail.redes2022.com.ar
correo   A      203.0.113.8
;
;
```

c. ¿Es necesario que el servidor de DNS acepte consultas recursivas? Justifique.

No es necesario, un servidor DNS puede contestar una consulta con la información que él "conoce", es decir una respuesta autoritativa. SI el emisor (quien hace la consulta) sabe quien és el que tiene la información podría hacerle una consulta iterativa a él, sin necesidad de que la consulta se delegue (consulta recursiva), obviamente esto sería hoy en dia inviable porque el emisor tendría que saber quien tiene cada dato, imposible. Pero en un caso concreto y sencillo se puede hacer.

d. ¿Qué servicios/protocolos de capa de aplicación configuraría en cada servidor?

- Dos servidores DNS: protocolo HTTP, HTTPS.
- Un servidor de correo electrónico: SMTP, POP3 e IMAP.
- Un servidor WEB para el acceso a un webmail : Se usa HTTPS.

e. Para cada servidor que puertos considera necesarios dejar abiertos a Internet. A modo de referencia, para cada puerto indique: Servidor, protocolo de transporte y número de puerto.

Servidor	**Protocolo de Transporte**	**Nº Puerto**
SMTP (Simple Mail Transport Protocol)	**TCP, UPD**	**25**
DNS (Domain Name System)	**TCP, UPD**	**53**
HTTP (HyperText Transfer Protocol)	**TCP**	**80**
POP3 (Post Office Protocol version 3)	**TCP**	**110**
IMAP, Interactive Mail AccessProtocol, version 3	**TCP, UPD**	**220**
HTTPS - HTTP Protocol over TLS/SSL	**TCP**	**443**
IMAP4 over SSL	**TCP**	**993**
POP3 over SSL	**TCP**	**995**

f. ¿Cómo cree que se conectaría el webmail del servidor web con el servidor de correo? ¿Qué protocolos usaría y para qué?

Con este servicio, el *agente de usuario* es un *navegador web corriente* y el usuario se comunica con su buzón remoto a través de HTTP. Cuando un destinatario “X”, desea acceder a un mensaje de su casilla de correos, éste es enviado desde el servidor de correo de “X” al navegador del mismo utilizando el protocolo HTTP en lugar de los protocolos POP3 o IMAP. Cuando un emisor, como “Y”, desea enviar un mensaje de correo electrónico, éste es transmitido desde su navegador a su servidor de correo a través de HTTP en lugar de mediante SMTP. Sin embargo, el servidor de correo de “Y”, continúa enviando mensajes a, y recibiendo mensajes de otros servidores de correo que emplean SMTP.

g. ¿Cómo se podría hacer para que cualquier MTA reconozca como válidos los mails provenientes del dominio redes2022.com.ar solamente a los que llegan de la dirección 203.0.113.111? ¿Afectaría esto a los mails enviados desde el Webmail? Justifique.

Un registro SPF determina qué servidores de correo y dominios tienen permitido enviar correo en nombre de tu dominio. Es una línea de texto sin formato que incluye una serie de etiquetas y valores. Las etiquetas se denominan *mecanismos*. Los valores suelen ser direcciones IP y nombres de dominio.
Así, los servidores que reciben correo consultan tu registro SPF para verificar que los mensajes entrantes que parecen ser de tu organización se hayan enviado desde servidores que has autorizado.
Los dominios solo pueden tener un registro SPF, pero en él se pueden especificar varios servidores y terceros que tengan permitido enviar correo en nombre del dominio en cuestión.
¿Cómo se configura?
Este protocolo se configura mediante el registro TXT (DNS) y como norma general tiene el siguiente aspecto:

Una vez explicado cómo funciona SPF, entonces en definitiva lo que debe realizar el administrador del domoinio redes2022.com.ar es agregar el registro TXT en el archivo de zona:

`v=spf1 ip4:`**203.0.113.111** `~all`
Donde:
v define la versión usada de SPF (versión 1)
IP4 direcciones IP de la v4
~all desautoriza a las máquinas que no encajen en lo autorizado explícitamente

Cuando un registro SPF incluye `~all` (calificador de que se supera la autenticación con reservas), los servidores que reciben correo suelen aceptar los mensajes de remitentes que no figuran en el registro SPF, pero los marcan como sospechosos.

Para poder usar el de webmail habria que agregar:

`v=spf1 a:`mail.redes2022.com.ar `ip4:`**203.0.113.111** `~all`

En este caso el mecanismo “a” autoriza a los servidores de correo por su nombre de dominio.

h. ¿Qué característica propia de SMTP, IMAP y POP, hace que al adjuntar una imagen o un ejecutable sea necesario aplicar un encoding (ej. base64)?

La RFC 822 define que los mensajes tienen dos partes: un encabezado y un cuerpo. Ambas partes están representadas en texto ASCII. Originalmente, se suponía que el cuerpo era un texto simple. Este sigue siendo el caso, aunque RFC 822 ha sido aumentado por MIME para permitir que el cuerpo del mensaje lleve todo tipo de datos. Estos datos todavía se representan como texto ASCII, pero debido a que puede ser una versión codificada de, por ejemplo, una imagen JPEG, no es necesariamente legible por los usuarios humanos.

Los clientes de correo y los servidores de correo convierten automáticamente desde y a formato MIME cuando envían o reciben (SMTP/MIME) e-mails

MIME ("extensiones multipropósito de correo de internet") son una serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario. Una parte importante del MIME está dedicada a mejorar las posibilidades de transferencia de texto en distintos idiomas y alfabetos.

Prácticamente todos los mensajes de correo electrónico escritos por personas en Internet y una proporción considerable de estos mensajes generados automáticamente son transmitidos en formato MIME a través de SMTP. Los mensajes de correo electrónico en Internet están tan cercanamente asociados con el SMTP y MIME que usualmente se les llama mensaje SMTP/MIME.

Los encabezados MIME son

- Content-Description: (Una descripción lejible para los humanos de qué hay en el mensaje)
- Content-Type: El tipo de data contenida en el mensaje (audio, video, image, application)
- Content-Transfer-Encoding: Cómo está codificado el cuerpo del mensaje(7bit, Quoted printable, base64, 8bit, binary)

i. ¿Se podría enviar un mail a un usuario de modo que el receptor vea que el remitente es un usuario distinto? En caso afirmativo, ¿Cómo? ¿Es una indicación de una estafa? Justifique

Los ataques de spoofing son aquellos en los que una persona intenta engañar al receptor falsificando sus datos, y existen varias categorías dependiendo de la tecnología que utilicen.

La categoría denominada email spoofing, que es un conjunto de técnicas utilizadas para hacerse pasar por otra persona o remitente en un correo electrónico. Esto es posible porque el protocolo SMTP (Simple Mail Transfer), que es el que se utiliza principalmente para el envío de correos electrónicos, no incluye un mecanismo de autenticación.

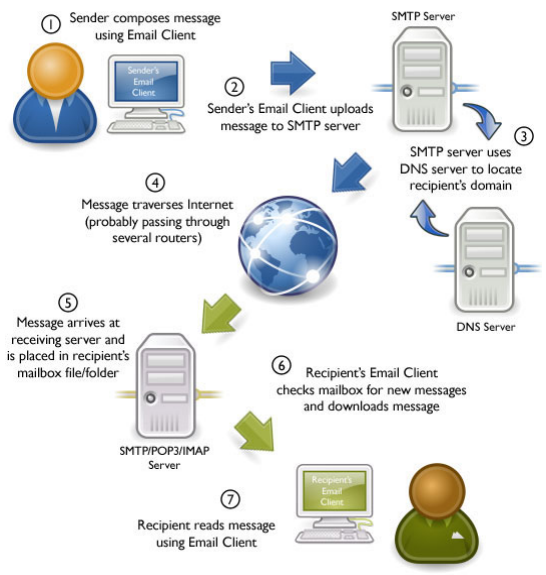
Esto quiere decir que cuando alguien te hace un email spoofing, recibirás un correo de un tal Juan o Marta, o de tu banco de referencia, pero que quien realmente no te ha enviado el correo no son ni Juan, ni Marta ni tu banco, sino otra persona que se está haciendo pasar por ellos. Esto suele hacerse con fines maliciosos como el phishing, intentando que te descargues algún malware o que les des datos personales o fiscales.

Puede hacerse enviando un correo por consola y dentro de DATA se agrega el campo “from” y se pone el nombre que queramos que el receptor vea.

j. ¿Se podría enviar un mail a un usuario de modo que el receptor vea que el destinatario es un usuario distinto? En caso afirmativo, ¿Cómo? ¿Por qué no le llegaría al destinatario que el receptor vé? ¿Es esto una indicación de una estafa? Justifique

Si, es posible, puede hacerse igual que en el inciso anterior, pero agregando el campo “to:”. No le llegaría al destinatario que el receptor ve porque el envelope (sobre) con el que se queda el MTA tiene el “mail to:” que nos indica el destinatario. Esto se lo queda el servidor y el destinatario lo que ve es la información contenida dentro de DATA. No creemos que pueda ser un indicio de estafa, debido a que cada uno tiene noción de quién es y no se logra el mismo efecto que cambiando el emisor y haciéndose pasar por alguien más.

k. ¿Qué protocolo usará nuestro MUA para enviar un correo con remitente redes@info.unlp.edu.ar? ¿Con quién se conectará? ¿Qué información será necesaria y cómo la obtendría?



Nuestro MUA envía un correo electrónico a través del agente de envío de correo/mensaje (MSA) el cual se lo envía a nuestro MTA mediante SMTP. El MTA, si el destinatario no está alojado localmente, consulta al servidor DNS cual es la IP del MTA del destinatario (redes@info.unlp.edu.ar) y una vez conseguida esta dirección le envía el email al MTA del receptor mediante SMTP. Luego llega al agente de entrega de correo (MDA). Esta es la última escala del correo electrónico antes de que se entregue al buzón del destinatario. El envío de correo electrónico se realiza mediante SMTP (o SMTP extendido), y para la etapa final (MDA a MUA), se utiliza POP3 o IMAP4.

l. Dado que solo disponemos de un servidor de correo, ¿qué sucederá con los mails que intenten ingresar durante un reinicio del servidor?

Si el servidor del emisor no puede enviar el mensaje de correo a nuestro servidor, entonces el servidor del emisor mantiene el mensaje en una cola de mensajes e intenta enviarlo más tarde. Normalmente, los reintentos de envío se realizan más o menos cada 30 minutos; si después de varios días no se ha conseguido, el servidor elimina el mensaje y se lo notifica al emisor mediante un mensaje de correo electrónico.

SMTP no utiliza servidores de correo intermedios para enviar correo, incluso cuando los dos servidores de correo se encuentran en extremos opuestos del mundo. Si nuestro servidor está en La Plata y el del emisor está en Tokyo, la conexión TCP será una conexión directa entre los servidores de La Plata y Tokyo. En particular, si nuestro servidor de correo está fuera de servicio, el servidor del emisor conservará el mensaje y lo intentará de nuevo (el mensaje no se deja en un servidor de correo intermedio).

m. Suponga que contratamos un servidor de correo electrónico en la nube para integrarlo con nuestra arquitectura de servicios.

i. ¿Cómo configuraría el DNS para que ambos servidores de correo se comporten de manera de dar un servicio de correo tolerante a fallos?

Cuando se habilita la Tolerancia a Fallos para un determinado Servidor, se crea una imagen en vivo ejecutándose en otro servidor. Los dos servidores actúan conjuntamente ejecutando el mismo conjunto de eventos ya que reciben las mismas entradas en un determinado instante de tiempo.

De cara al exterior los dos servidores virtuales aparecen como una misma entidad con una única dirección IP y disco duro virtual, siendo el primario el único que puede escribir sobre dicho disco. Continuamente, los servidores se mandan pulsos entre ellos y, en el momento que se pierde la conectividad, el secundario pasa a realizar tareas de primario. Estos pulsos se envían en intervalos de milisegundos consiguiendo que la tolerancia a fallos sea instantánea.

Para que eso suceda, se agregará un nuevo registro MX a su información DNS, apuntando al servidor de correo de la nube con una prioridad más alta. Por ejemplo:

Registro FQDN	tipo registro	valor	MX Preferencia
mail.redes2022.com.ar	A	203.0.113.111	
mail.nube.com	A	ip servidor de la nube	
redes2022.com.ar	MX	mail.redes2022.com.ar	10
redes2022.com.ar	MX	mail.nube.com	100

*Un registro FQDN es un nombre de dominio completo que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo.

ii. Para pensar: ¿Cómo configuraría el DNS para que ambos servidores brinden un servicio de correo que balancee su carga entre los 2 servidores? Mencione algún protocolo que podría usarse para asegurar que sin importar por cuál mail server ingresen los mails, el webmail los verá de manera unificada.

El balance de carga de correo entrante , podría ser necesario si tuviésemos mucho tráfico de correo para recibir por hora y **un solo servidor** haciendo cola y procesando todos estos correos electrónicos, el cual eventualmente podría agotarse. Al implementar múltiples servidores MX podemos distribuir uniformemente la carga de correo electrónico entrante a todos ellos. Si hay una carga pesada como en los ataques de spam, la entrega de correo se retrasará y puede ocurrir la pérdida de correo electrónico. Para superar estas situaciones, debemos equilibrar la carga del flujo entrante a los otros servidores para un procesamiento rápido y una entrega más fluida.

Para balancear la carga de ambos servidores:

Habiendo agregado el servidor de correos de la nube y configurado el registro MX del DNS, para que apunte al servidor de correo, se debe modificar la prioridad, para que todos tengan la misma prioridad. Si dejamos el valor de preferencia igual, el de la nube más alto que el primer servidor de correos, esto provocaría que el primer servidor tenga que resolver todas las consultas, al no tener preferencia por ningún servidor de correo, se logra una división de las consultas pareja.

Siguiendo con el cuadro del inciso anterior:

Registro FQDN	Tipo registro	Valor	MX Preferencia
mail.redes2022.com.ar	A	203.0.113.111	
mail.nube.com	A	IP Servidor de la nube	
redes2022.com.ar	MX	mail.redes2022.com.ar	10
redes2022.com.ar	MX	mail.nube.com	10

Balance de correo electrónico con round-robin DNS:

Este método puede utilizarse para 2 servidores, como en nuestro caso y resulta escalable ya que podrían agregarse nuevos servidores.

Para que el round-robin DNS funcione, tenemos que declarar la misma prioridad para todos los registros MX. Si todos tienen el mismo valor de prioridad, el DNS envía las IPs del servidor rotando, como es característica del round-robin. Al momento en que un emisor de mensaje consulte a nuestro server DNS cuál es nuestro servidor de mail, la respuesta del DNS irá rotando entre nuestros servidores de correo.