Registro SPF: asegura la entrega de tus emails

Todos estaréis de acuerdo con nosotros en que hoy el día el correo electrónico es una herramienta que nos facilita mucho la comunicación entre usuarios. Pero como suele ocurrir en otras situaciones, este aumento del uso del email ha traído consigo la aparición de importantes problemas, siendo uno de los más habituales la falsificación de la dirección del remitente.

Las víctimas cuyas direcciones están siendo utilizadas para hacer el fraude son las que sufren las consecuencias, ya que su reputación online se ve afectada, llegando a tener problemas a la hora de realizar envíos a otros destinatarios, debido a que los mensajes enviados desde esas direcciones son consideradas como mensajes potencialmente peligrosos por los sistemas antispam de los proveedores de servicios.

Probablemente algunos de vosotros habréis experimentado este tipo de problemas, por ejemplo cuando recibimos algún correo de error indicándonos que un mensaje no pudo ser entregado al destinatario, aunque nunca llegamos a enviar ese correo.

Para poner fin a este problema se desarrolló una solución a nivel de registros de DNS. Nos estamos refiriendo al registro de texto SPF.

Qué es el registro SPF

El registro SPF (Sender Policy Framework) es actualmente uno de los protocolos más utilizados en la actualidad para luchar contra el spam o el correo basura. Se trata de un registro DNS que se activa dentro de la zona de DNS del dominio de origen.

Básicamente, la aparición de este registro dentro del dominio que realiza el envío del correo permite al servidor que recibe el correo electrónico comparar el dominio con la lista de los equipos que están autorizados para realizar el envío de mensajes desde dicho dominio. En base a ese registro, el servidor toma las decisiones oportunas para determinar si dejar pasar el correo y entregarlo al destinatario o bien bloquearlo.

La activación de este tipo de registro no es complicada. Lo único que hay que hacer es acceder al servidor de DNS y una vez allí crear un registro de este tipo, indicando una serie de parámetros que harán que el servidor de correo actúe de una forma u otra cuando reciba un correo con SPF activo y lo valide.

Cómo comprobar si tenemos un registro SPF activado

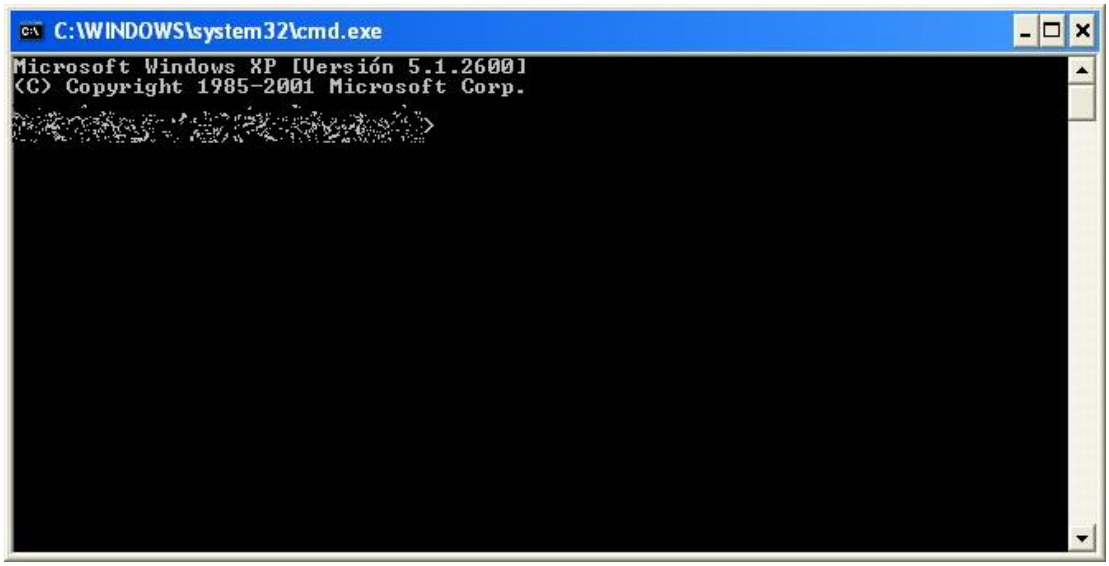
A la hora de ver si nuestro dominio tiene configurado este tipo de registros, se puede hacer de varias maneras. La más rápida es acceder a la zona de DNS del proveedor donde está registrado el dominio y asegurarnos que hay una entrada de tipo TXT.

[redacted]	TXT	v=spf1 redirect=spf.dominioabsoluto.net	
[redacted]	A	82.194.88.7	
[redacted]	A	217.116.0.237	
[redacted]	A	82.194.88.7	
[redacted]	A	217.116.0.227	

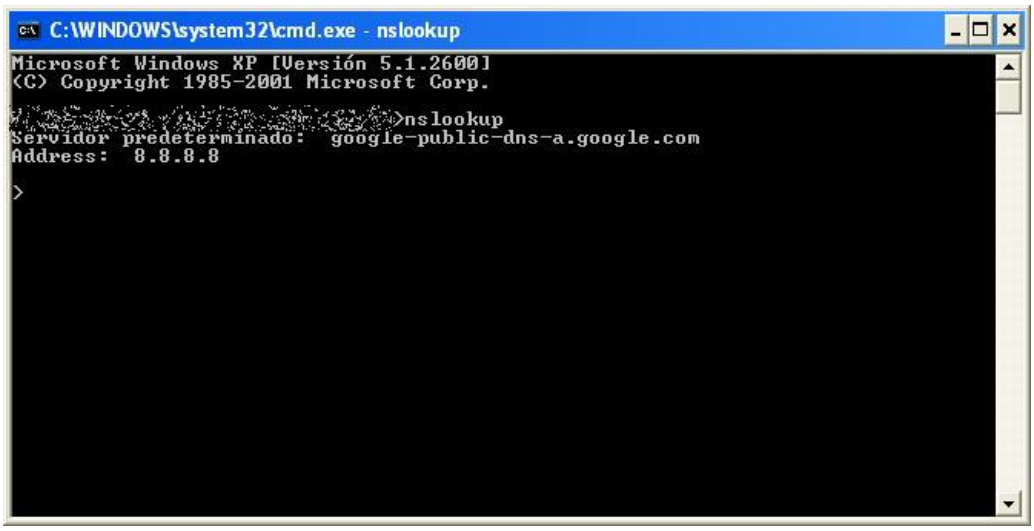
Veamos ahora otras formas de revisar este registro.

1.- Desde consola de Windows

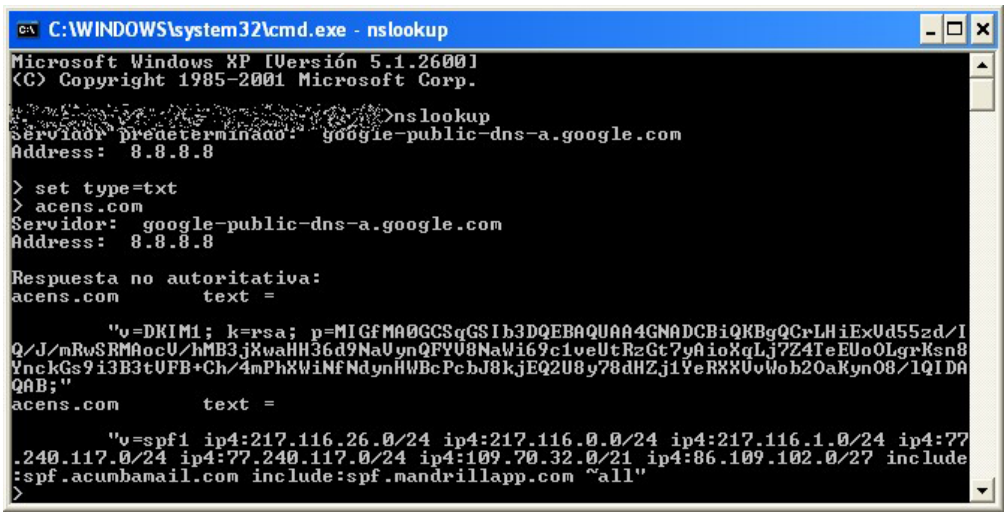
En este caso, lo primero que debemos hacer es pulsar en Inicio y en el recuadro "Buscar programas y archivos" escribimos "cmd". Esto nos abrirá un terminal desde donde ejecutar los comandos. En nuestro caso haremos una prueba con nuestro dominio acens.com.



A continuación escribimos "nslookup" y pulsamos Enter.



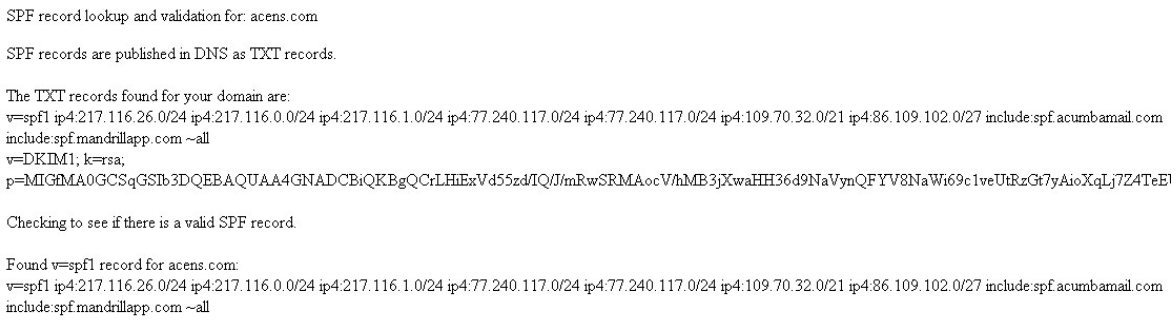
Tecleamos “set type=txt”, pulsamos Enter y después escribimos el nombre del dominio, en nuestro caso “acens.com”. De nuevo pulsamos Enter. Una vez hecho todo esto, deberíais ver algo similar a lo que muestra la siguiente pantalla.



2.- Comprobación online

Otra forma de comprobar que está creado el registro SPF en nuestro dominio, es hacer uso de algunas de las herramientas online que nos podemos encontrar. Una de ellas es la que nos ofrece la página Kitterman.

Una vez dentro, tecleamos el nombre de nuestro dominio y pulsamos en el botón “Get SPF Record” para poder ver el valor de este registro si estuviera creado.


SPF record lookup and validation for: acens.com

SPF records are published in DNS as TXT records.

The TXT records found for your domain are:
v=spf1 ip4:217.116.26.0/24 ip4:217.116.0.0/24 ip4:217.116.1.0/24 ip4:77.240.117.0/24 ip4:77.240.117.0/24 ip4:109.70.32.0/21 ip4:86.109.102.0/27 include:spf.acumbamail.com include:spf.mandrillapp.com ~all
v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrLHiExVd55zd/IQ/J/mRwSRMAocV/hMB3jXwaHH36d9NaVynQFYV8NaWi69c1veUtRzGt7yAioXqLj7Z4TeE

Checking to see if there is a valid SPF record.

Found v=spf1 record for acens.com:
v=spf1 ip4:217.116.26.0/24 ip4:217.116.0.0/24 ip4:217.116.1.0/24 ip4:77.240.117.0/24 ip4:77.240.117.0/24 ip4:109.70.32.0/21 ip4:86.109.102.0/27 include:spf.acumbamail.com include:spf.mandrillapp.com ~all

Configurar el registro SFP

Como hemos comentado anteriormente este registro debe ser añadido en la configuración de la zona de DNS del dominio en cuestión, utilizando para ello los registros de tipo TXT que nos encontraremos en el apartado de configuración de registros de DNS.

A la hora de realizar la configuración de este registro, deberemos hacer uso de las variables que nos ofrece el registro SFP. A continuación podéis ver un ejemplo de registro SPF.

v=spf1 ip4:5.57.100.0/24 mx -all

Antes de meternos en su explicación, decir que todo registro SPF debe empezar por el campo “v” que sirve para indicar la versión que vayamos a utilizar.

Para definir el SPF nos valemos de dos elementos: mecanismos y prefijos

Mecanismos

En el registro SPF pueden aparecer cero o más mecanismos que son utilizados para describir el grupo de hosts asignados como emisores de correo para ese dominio. Los mecanismos que se pueden utilizar son los siguientes:

- all
- a
- mx
- ptr
- ip4
- ip6
- include

Estos mecanismos pueden llevar los siguientes prefijos.

- **-** (guión medio). Se conoce como el prefijo fail y al utilizarlo dentro de un mecanismo, estaríamos rechazando la dirección IP que formara parte de ese mecanismo, desechando el mensaje procedente de esa dirección.
- **~** (virgulilla). En este caso se conoce como Softfail. El mensaje procedente de la dirección IP indicada no sería rechazado pero se marcaría su cabecera de forma especial para darle un tratamiento posterior.
- **+**. Se conoce con el nombre de Pass y lo que hace es aprobar la dirección IP que lo acompaña.
- **?**. Se trata del prefijo Neutral y es un prefijo que se utiliza en periodos de prueba. En este caso el mensaje no se daría como bueno pero tampoco como malo, sino que se añadiría en su cabecera la instrucción Received-SPF: neutral.

Pasemos a explicar cada uno de los mecanismos que podemos utilizar para la creación del registro SPF.

1. all

Se trata de un mecanismo que se suele poner al final del todo. Lo normal es ponerle el prefijo - o ~ para desautorizar cualquier petición que no haya coincidido con los mecanismos anteriores. Un ejemplo de uso podría ser el siguiente.

v=spf1 -all

2. a

Mediante este mecanismo estamos indicando los servidores que podrán enviar mensajes con nuestro dominio, indicando que podrán hacerlo aquellas direcciones IPs asociadas a los registros de tipo A del dominio en cuestión.

Si no se indica el nombre del dominio asociado al mecanismo “a”, se utiliza el dominio asociado a la dirección de correo electrónico para hacer la consulta de los registros A.

Algunos ejemplos de uso de este mecanismo pueden ser:

v=spf1 a –all
v=spf1 a:ejemplo.com -all

3. mx

Se trata de un mecanismo similar al anterior, pero en este caso estamos indicando que lo podrán hacer aquellas direcciones IP que estén asociadas a los registros mx del dominio. Como en el caso anterior, sino se indica el nombre del dominio, se cogerá el nombre de la dirección de correo del envío.

v=spf1 mx -all
v=spf1 mx:ejemplo.com -all

4. ptr

Mediante este mecanismo estamos indicando que podrán realizar el envío aquellas direcciones IPs cuya resolución inversa pertenezca al dominio en cuestión. Como en los casos anteriores, si no se especifica nombre de dominio, se utiliza el propio de la dirección del correo.

v=spf1 mx –all
v=spf1 mx:ejemplo.com ptr:nuevodominio.com -all

5. ip4

Al utilizar este mecanismo estamos indicando que se acepten aquellos correos que son enviados desde la dirección IP o que pertenezca al rango indicado. La dirección IP no tiene por qué coincidir con la IP del dominio.

v=spf1 a:ejemplo.com ip4:192.168.0.1 -all
v=spf1 a:ejemplo.com ip4:192.168.0.1/16 -all

6. ip6

Funciona de la misma forma que el caso de ip4 pero en este caso con las nuevas direcciones ip6.

v=spf1 a:ejemplo.com ip4:192.168.0.1 ip6:2001:0DB8:AC10:FE01 -all

7. include

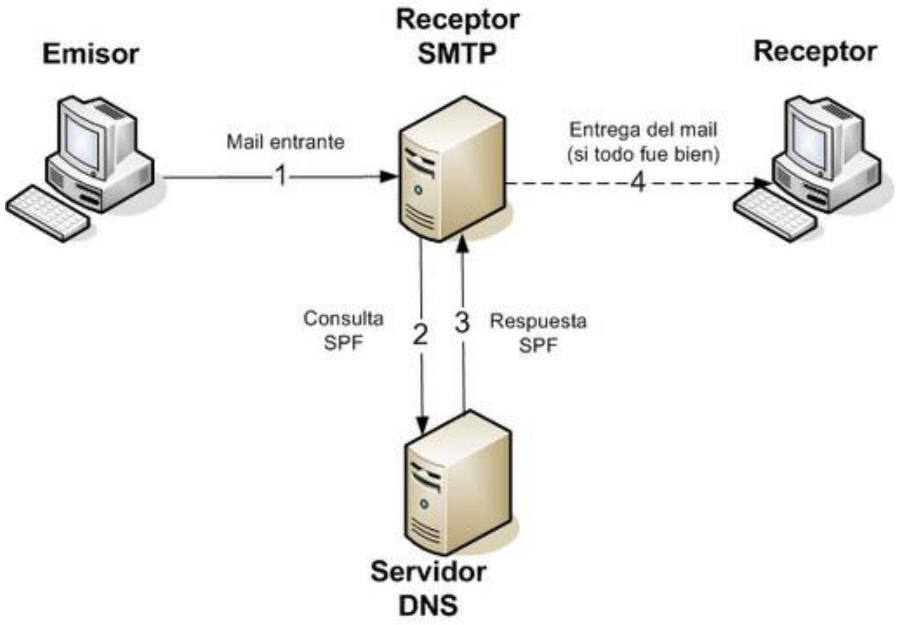
Con este mecanismo, lo que estamos indicando es que busque en otro dominio un mecanismo que devuelva el valor “permitido” que garantice que el email es correcto y debe ser aceptado. Si la consulta a este nuevo dominio no devuelve “permitido”, el proceso pasa a la siguiente directiva del registro SPF.

v=spf1 include:otrodominio.net a:ejemplo.com -all

En el ejemplo anterior, mira primero el registro SPF del dominio otrodominio.net. Si en alguna de las directivas que forman parte de él se obtiene el valor “permitido”, el correo es aceptado. Si por el contrario no se consigue ese valor, entonces se pasaría a analizar el siguiente mecanismo, que en nuestro caso de ejemplo sería “a:ejemplo.com”.

Al utilizar include hay que tener en cuenta que si el dominio que indiquemos no tiene un registro SPF correcto, se retornará un error permanente.

Funcionamiento



Como ya hemos comentado, el objetivo de utilizar este tipo de registros es verificar al servidor que recibe el correo electrónico que el destinatario es correcto y que no se trata de ningún tipo de suplantación de identidad o cosa similar. El servidor de correo que recibe el mensaje analiza el registro SPF que pueda tener el dominio que envía el correo en busca de un mecanismo que le garantice que es correcto. Para ello, se siguen las siguientes reglas:

- Si no se indica ningún tipo de prefijo, el que se utiliza por defecto es pass (+).
- La evaluación de los mecanismos se realiza en orden, de izquierda a derecha hasta que se encuentra alguna coincidencia entre el mecanismo y la dirección IP del emisor. Una vez encontrada esa coincidencia entra en juego el valor del prefijo que lo acompaña para determinar si el mensaje será aceptado o denegado.
- Si un dominio no tiene registro SPF, el valor que toma la comprobación del SPF es 'none', aceptando el servidor de destino el correo enviado.