

Sender Policy Framework en MDaemon 7.1+

Alt-N Technologies, Ltd
2201 East Lamar Blvd, Suite 270
Arlington, TX 76006
Tel: (817) 525-2005

© 2004 Alt-N Technologies. Reservados todos los derechos.

Los nombres de productos y empresas que se mencionan en este documento pueden ser marcas registradas.

Resumen

La suplantación de las direcciones de e-mail produce graves problemas en las comunicaciones por Internet. La suplantación es la utilización no autorizada de una dirección de e-mail. Es una de las técnicas habituales para difundir mensajes de correo basura, virus y otros tipos de engaños. Permite a los remitentes de los e-mails ocultar su verdadera identidad. Cualquiera puede suplantar fácilmente una dirección de e-mail modificando la dirección de retorno en la configuración de un cliente e-mail. El Sender Policy Framework (SPF) es un protocolo de seguridad abierto diseñado para detectar direcciones de e-mail suplantadas. Es un elemento importante en la política de seguridad del e-mail. El SPF verifica las identidades de los servidores de e-mail para los mensajes entrantes. Compara la dirección e-mail REMITENTE de un mensaje contra una lista de todos los ordenadores autorizados para enviar e-mails a esa dirección. Con los resultados de la búsqueda del SPF, un servidor de e-mail (o otro software) que trabaje con SPF puede realizar las acciones adecuadas. En la versión 7.1, MDaemon ofrece SPF entre sus opciones de seguridad.

Algunos conceptos sobre SPF

Sobre la suplantación de direcciones

La suplantación en las direcciones de e-mail permite la amplia proliferación de correo basura y virus ocultando la verdadera identidad de sus responsables.

Los suplantadores utilizan direcciones de e-mail de otras personas sin su permiso ni conocimiento. De este modo, cualquier persona puede enviar e-mails pretendiendo ser otra persona. Por ejemplo, alguien puede enviar mensajes haciéndose pasar por:

Los orígenes del envío flexible de e-mails

La suplantación en los envíos de e-mails es posible debido a la flexibilidad, transparencia y confianza de los sistemas de correo electrónico actuales. La idea es sencilla- permitir a los usuarios enviar e-mails desde diferentes servidores y recibir correo en una dirección consolidada.

A la práctica, este concepto de diseño resulta muy útil para algunos usuarios de e-mail. Pongamos como ejemplo a los viajeros:

Muchas personas tienen que viajar como parte de su trabajo. Por diferentes motivos –principalmente de seguridad- su servidor de e-mail puede no estar disponible para enviar mensajes desde otras ubicaciones. Como alternativa, los viajeros pueden enviar sus e-mails mediante servicios públicos como Hotmail o Yahoo!, proveedores de Internet como Earthlink o servidores de e-mail personal en sus ordenadores portátiles. También pueden utilizar una combinación de todos estos, según sus necesidades, preferencias, y la disponibilidad de los servicios en las diferentes partes del mundo.

En cualquier caso, sea cual sea el método que elijan para enviar los mensajes, los viajeros suelen incluir su información de correo personal como dirección de respuesta. De esta manera pueden recibir todos sus mensajes en una sola cuenta de e-mail.

Cada día, miles de usuarios aprovechan el e-mail para enviar mensajes desde un dominio y los reciben en otro, por razones absolutamente legítimas. Más a menudo todavía, spammers, creadores de virus y ladrones aprovechan la fragilidad del correo con intenciones inadecuadas e ilegales.

Repercusiones de la suplantación

La suplantación en las direcciones de e-mail contribuye en la rápida expansión de correo basura, virus y al robo de información.

Los spammers a menudo se ocultan tras direcciones de respuesta suplantadas. Responder o rebotar el mensaje suele resultar en un mensaje "Returned mail: User unknown". El coste del

correo basura asciende a millones anuales en tiempo perdido, ancho de banda robado, y recursos informáticos malgastados. El correo basura no proporciona beneficios, excepto a los spammers. Por este motivo, el correo basura es conocido por lo barato que resulta a quienes lo envían y lo caro que es para el resto de personas.

Los virus suelen expandirse mediante direcciones reales, pero suplantadas, que obtienen de los equipos de sus víctimas. Muchos virus envían mensajes utilizando sus propios remitentes de e-mail implementados. Se auto-envían a todas las direcciones que encuentran en los equipos infectados. También suplantando aleatoriamente la dirección de los remitentes del mensaje. A parte de expandir virus, este método genera una avalancha de mensajes “Se han detectado virus” a la dirección suplantada. Esto confunde a algunos usuarios que responden enfadados, malgastando más tiempo y recursos. Los virus también pueden infectar equipos que disponen de software diseñado para lanzar ataques de denegación de servicio.

Los ciber-timadores se sirven de la suplantación para hacerse pasar por personas que necesitan saber, por motivos legítimos, informaciones personales. Por ejemplo, un e-mail que solicite información sobre la cuenta, puede parecer que provenga del administrador del sistema. En cambio, la dirección ha sido suplantada y la respuesta la recibirá un gamberro que busca el acceso no autorizado. En otro tipo de estafa, un e-mail solicita al usuario que actualice la información de su cuenta en un servicio financiero on-line. Aunque las credenciales del e-mail puedan parecer auténticas, la información actualizada ayuda a los ladrones de identidades.

Debido al aumento de las suplantaciones, la falsificación de direcciones de e-mail ha aumentado. Más del 50 % de los mensajes de e-mail utilizan direcciones de respuesta suplantadas. En realidad, el volumen de correo ilegal e indeseado es suficientemente elevado para amenazar la utilización legítima del e-mail.

Dificultar la suplantación de direcciones obliga a los spammers a utilizar sus propias direcciones de e-mail. Si se detiene la falsificación de e-mails, se detiene también uno de los medios principales de expandir virus. Cuando los spammers y creadores de virus no puedan seguir suplantando direcciones, sus mensajes no deseados serán fácilmente detectables y se podrán bloquear con otras medidas de seguridad.

Medidas de seguridad y suplantación

Hasta hace poco, no existían medidas estrictas para prevenir la suplantación de remitentes de e-mails.

Los expertos en seguridad de e-mails -con Alt-N Technologies- han desarrollado numerosos sistemas para detectar y eliminar mensajes no deseados y peligrosos. Estas técnicas consisten básicamente en prevenir el uso no autorizado de servidores de e-mail y el bloqueo de mensajes no deseados.

Algunos métodos requieren una intervención humana periódica, en la revisión del feedback de los usuarios y la lectura de los archivos del sistema. Otros enfoques apuestan por el software de análisis, la detección y la intervención preventiva. A su vez, algunos usuarios han implementado firmas digitales encriptadas para la identificación positiva del usuario.

MDaemon— líder del sector en la protección de servidores de e-mail y usuarios de cuentas—dispone de diferentes recursos de seguridad que incluyen:

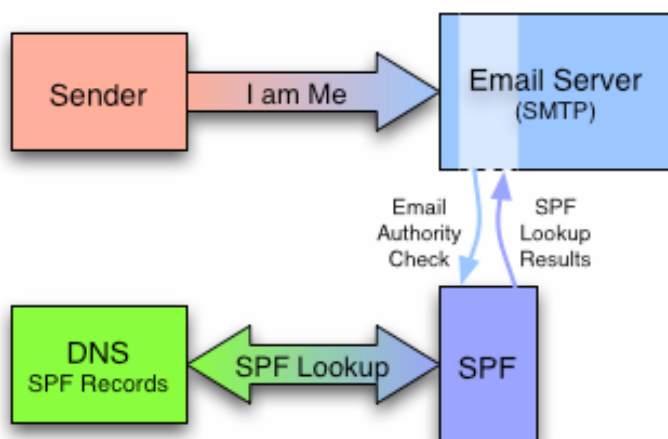
Antivirus	Adjuntos restringidos	Supresión de dirección
-----------	-----------------------	------------------------

Filtro de contenido	Control de retransmisión	Análisis de IP
Bloqueo de correo basura	IP de confianza	Análisis del host
Filtro anti correo basura	Tarpitting	Protección de IP
SSL	Búsquedas invertidas	AUTH
TLS	Dominios de confianza	POP previo a SMTP

Aunque estas opciones de seguridad tratan cuestiones generales y específicas, ninguna afecta específicamente al problema de la suplantación de direcciones de e-mail. Aquí se aplica el Sender Policy Framework.

Fundamentos del SPF

El Sender Policy Framework detecta las direcciones de e-mail suplantadas. Las detecta comprobando la validez de las direcciones de los remitentes en los sobres de los mensajes. Si un sobre contiene una dirección de remite suplantada, el mensaje puede ser rechazado. Esto ahorra tiempo de procesamiento y ancho de banda porque el servidor no descarga el mensaje. Sin embargo, aunque una dirección haya sido suplantada, el mensaje puede llegar a descargarse para un procesamiento adicional, e incluso, puede llegar a ser entregado.



El servidor de e-mail pausa el procesamiento de un mensaje mientras SPF valida la dirección remitente contra los servidores de e-mail autorizados de un dominio. La expansión del SPF contribuirá en la reducción de la cantidad de correo basura, virus y e-mails no deseados deteniendo la suplantación de e-mails.

El concepto de SPF se creó a finales de los años noventa. SPF es una versión simplificada de la propuesta RMX de Hadmut Danisch. RMX se basa en el artículo de Paul Vixie, *Repudiating Mail-From*. El artículo de Vixie fue el resultado de una sugerencia de Jim Miller en 1998.

Registros de SPF

La información de esta sección destaca los conceptos de registro del SPF. Para más información, ver SPF RFC en: <http://spf.pobox.com/rfcs.html>

SPF utiliza registros DNS especiales. Estos registros identifican SMTP autorizados para cada dominio. También pueden especificar otros dominios utilizados por los usuarios de las cuentas de e-mail.

Un registro SPF consta del número de versión SPF, seguido por los datos que incluyen mecanismos, prefijos y modificadores. El formato genérico es el siguiente:

Una entrada de ejemplo se parecería a:

En el ejemplo:

	es el número de versión. Hay una.
	son mecanismos. Pueden existir uno o más mecanismos.
	son prefijos. Los prefijos preceden a los mecanismos —si no se especifican + se implica.
	es un modificador. Pueden ser cero, uno o dos modificadores.

Número de versión

Un registro SPF siempre empieza con el número de versión, como

Las versiones posteriores podrían ser:

La versión designa el nivel de SPF soportado por el registro.

Mecanismos

Los mecanismos identifican las direcciones IP autorizadas para enviar e-mails desde un dominio. Dos mecanismos *básicos* — y —generalmente se relacionan con amplias categorías de IP, internas y externas en un dominio. El resto de mecanismos —como , y —autorizan la IP del remitente. Los mecanismos especifican:

	Todas las IP, locales y remotas.
	dominios externos utilizados por los remitentes de e-mails locales, habituales cuando viajan.
	todas las IP del registro DNS A.
	todos los registros A de cada registro host MX.
	todos los registros A de los registros host PTR.
	Uno o más dominios especificados que utilizan Ip IPv4.
	Uno o más dominios especificados que se identifican como excepciones de las definiciones SPF.

Prefijos

Mientras que los mecanismos identifican las direcciones IP, los prefijos designan si o no las direcciones IP superan o no los tests de búsqueda.

El mecanismo es una aplicación frecuente de los prefijos. Cuando aparece en un registro SPF, significa que ninguna IP supera el test¹.

¹ A la práctica, significa que ninguna otra IP supera el test. Los clientes SPF, como MDAemon, leen y procesan los elementos de los registros SPF de izquierda a derecha. Los estándares SPF recomiendan cerrar la mayoría de registros SPF con . Esto detiene el proceso de registro de SPF porque no se comprueba ninguna otra IP.

Los prefijos designan si una IP supera o no los tests de búsqueda. Por ejemplo:

	la dirección ha superado el test. Ejemplo:
	la dirección ha suspendido el test. Ejemplo:
	la dirección ha suspendido el test pero el resultado no es definitivo. Ejemplo:
	La dirección no ha superado o ha suspendido el test. Ejemplo:

El prefijo + es el predeterminado para todos los mecanismos. Por ejemplo, es igual a

Modificadores

Los modificadores ofrecen información adicional. También pueden bifurcar el procesamiento de SPF:

SPF cuenta con dos modificadores habituales:

	Envía la consulta de SPF a otro dominio. Ejemplo:
	Incluye una explicación en el registro SPF. Ejemplo:

Ejemplos de registros de SPF

A continuación se muestran algunos ejemplos sencillos de posibles registros SPF.

	Indica que ninguna dirección supera el test.
	Indica que todas las direcciones superan el test.
	Indica que las direcciones listadas en el registro DNS A superan el test.
	Indica que las direcciones listadas en el registro MX A superan el test.
	Indica que las direcciones listadas en el registro DNS, MX y PTR A superan el test.
	Indica una única dirección IP o una serie de IP que superan el test.

Para visualizar un registro SPF, use la orden desde la ventana terminal. Por ejemplo, para visualizar el registro Alt-N SPF, debe teclear y pulsar Intro:

Voluntary Deployment

Registrar información SPF en registros DNS es una nueva opción voluntaria para remitentes de e-mails. Muchas grandes empresas como Amazon, AOL, Earthlink, Google y Symantec utilizan SPF. SPF es uno de los métodos más utilizados para validar los remitentes de mensajes. Cuantos más dominios utilicen SPF, mejor será su funcionamiento.

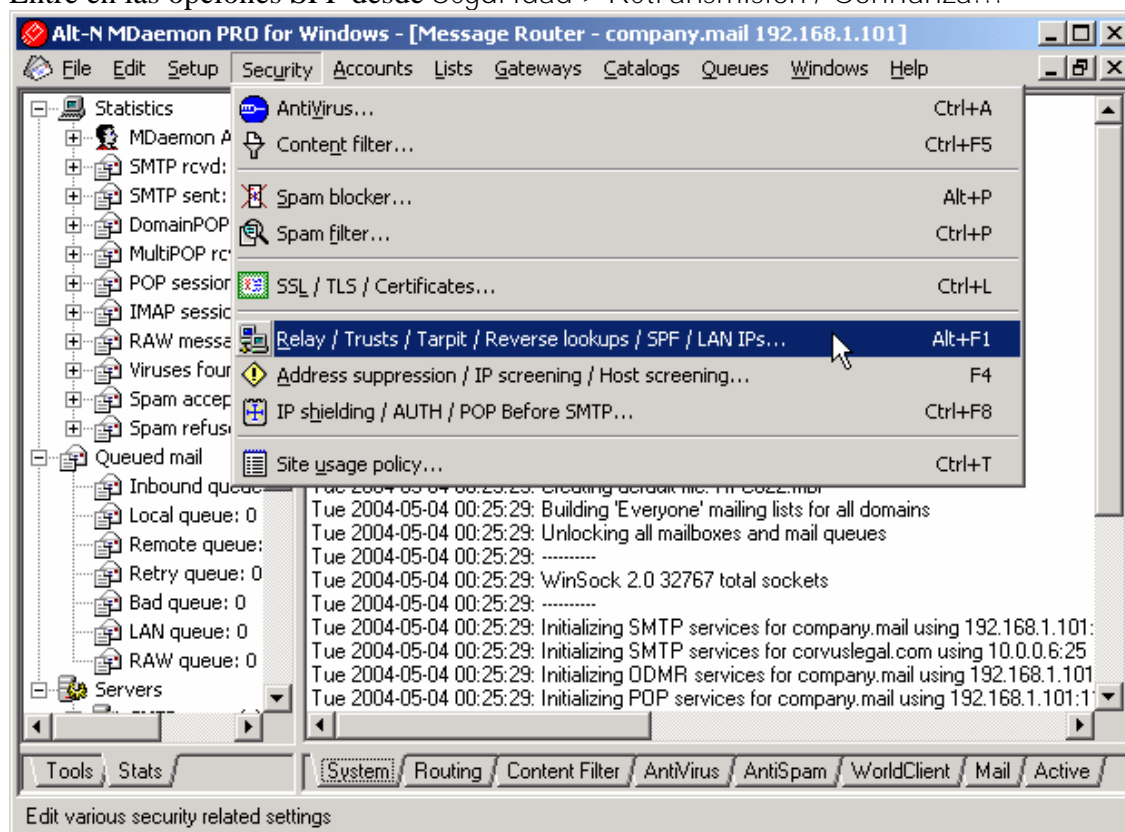
Implementación de SPF en MDAemon

Cliente SPF

A partir de la Versión 7.1, MDAemon puede servir como cliente SPF. Esto implica que puede comprobar la información SPF. Según el resultado de la búsqueda SPF, MDAemon puede rechazar un mensaje, ahorrando ancho de banda y espacio en disco. También puede pasar el mensaje al filtro de contenido o al filtro de correo basura, por ejemplo, para un posterior análisis. Los resultados de SPF pueden establecer también valores de probabilidad de correo basura para los mensajes.

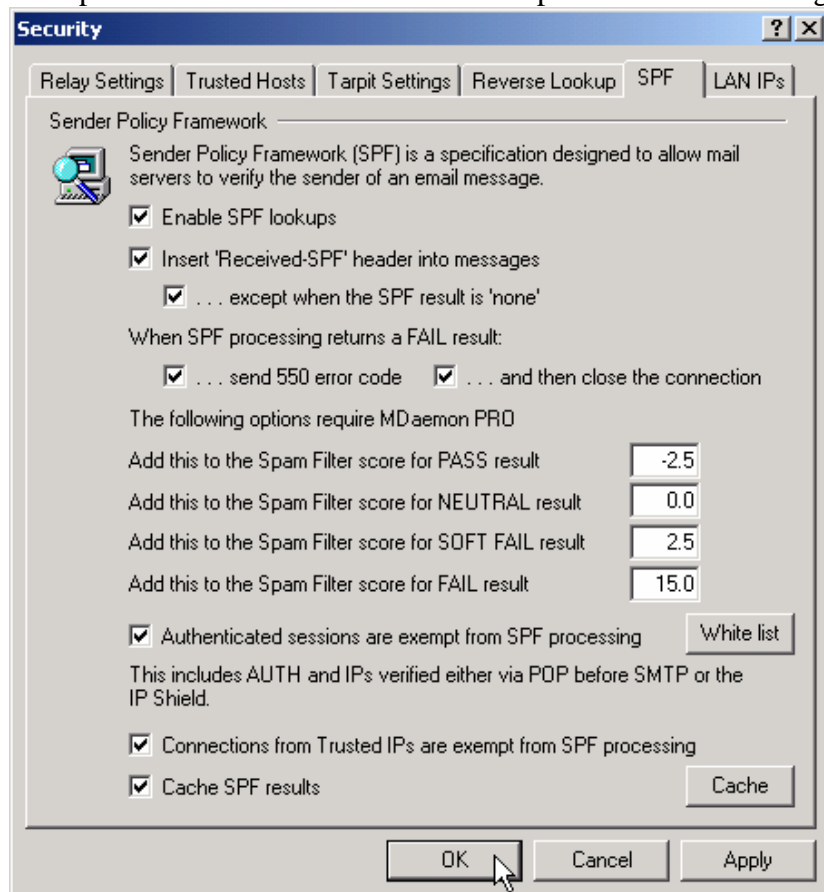
Orden SPF

Entre en las opciones SPF desde Seguridad > Retransmisión / Confianza...



Opciones de SPF

Las opciones de SPF se encuentran en la pestaña SPF del diálogo Seguridad.



Las opciones de este diálogo son:

Habilitar búsquedas SPF

Activar para permitir que MDAemon compruebe los registros SPF.

Insertar encabezado 'Received-SPF' en los mensajes

Activar para insertar encabezados SPF en los mensajes entrantes. Los encabezados describen los resultados de las búsquedas de SPF.

Por ejemplo, este es el encabezado de un mensaje de un dominio sin registro SPF:



Este encabezado es de un mensaje de un dominio con registro SPF:



Activando ...excepto cuando el resultado SPF es "none", evita que MDAemon añada el encabezado a los mensajes de dominios sin registro SPF.

Cuando el procesamiento SPF resulta en FALLO:

Activar enviar código de error 550 para devolver una respuesta 'no existe tal cuenta' al remitente. **Activar** y cerrar la conexión para finalizar la sesión. Esto bloquea los mensajes y no volverán a entrar en su servidor.

Añadir valor en Filtro correo basura...

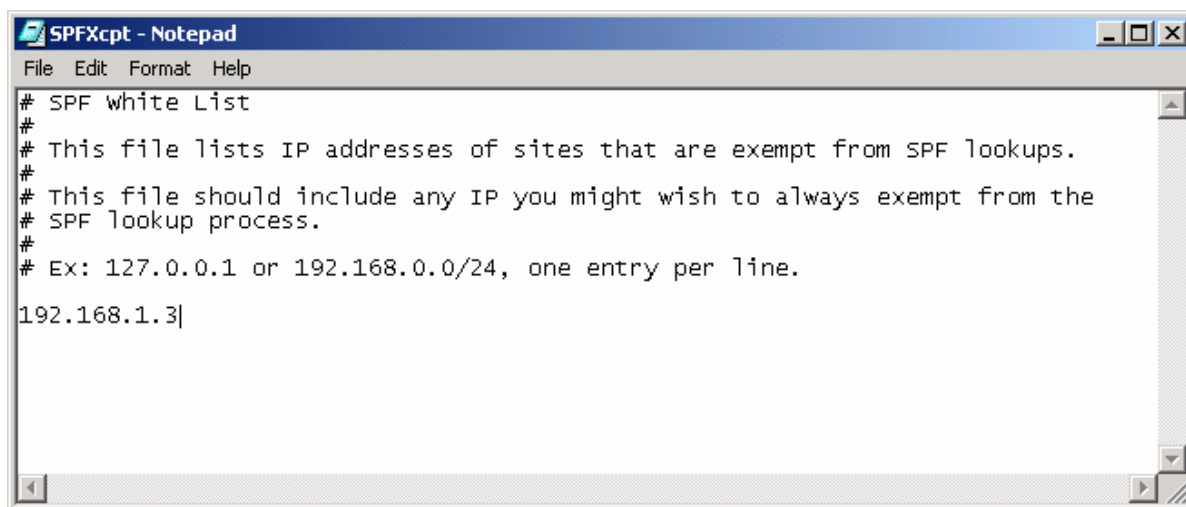
Estas opciones establecen el valor del Filtro de correo basura que se añadirá y restará, según los resultados SPF.

Las sesiones autenticadas están exentas de procesamiento SPF

Activar para evitar el procesamiento SPF de los mensajes que provienen de sesiones autenticadas.

Lista blanca

Seleccionar para abrir una ventana de edición y entrar una lista blanca de direcciones IP. Están exentas de procesamiento SPF.



Conexiones de IP de confianza exentas de procesamiento SPF

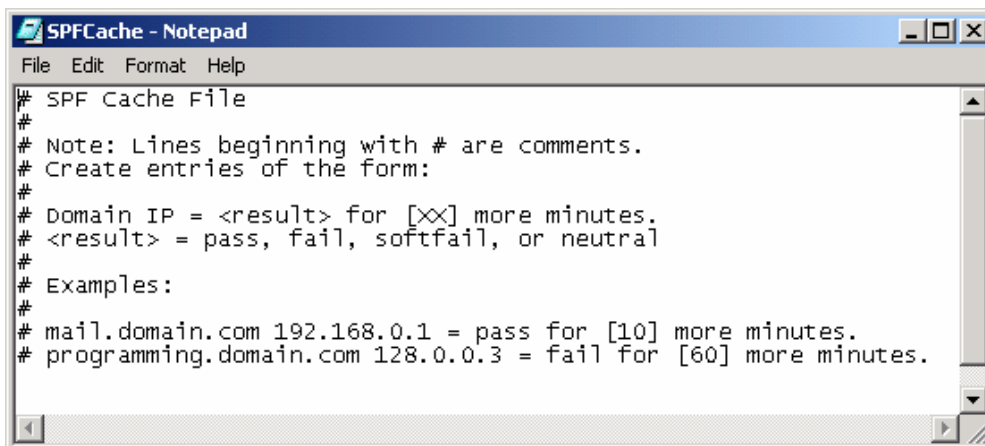
Activar para evitar el procesamiento SPF de los mensajes que provienen de una IP de confianza.

Resultados Caché SPF

Activar para mantener los resultados del procesamiento SPF durante un periodo de tiempo concreto.

Caché

Seleccionar para abrir una ventana de edición y entrar en la información de la caché de SPF.



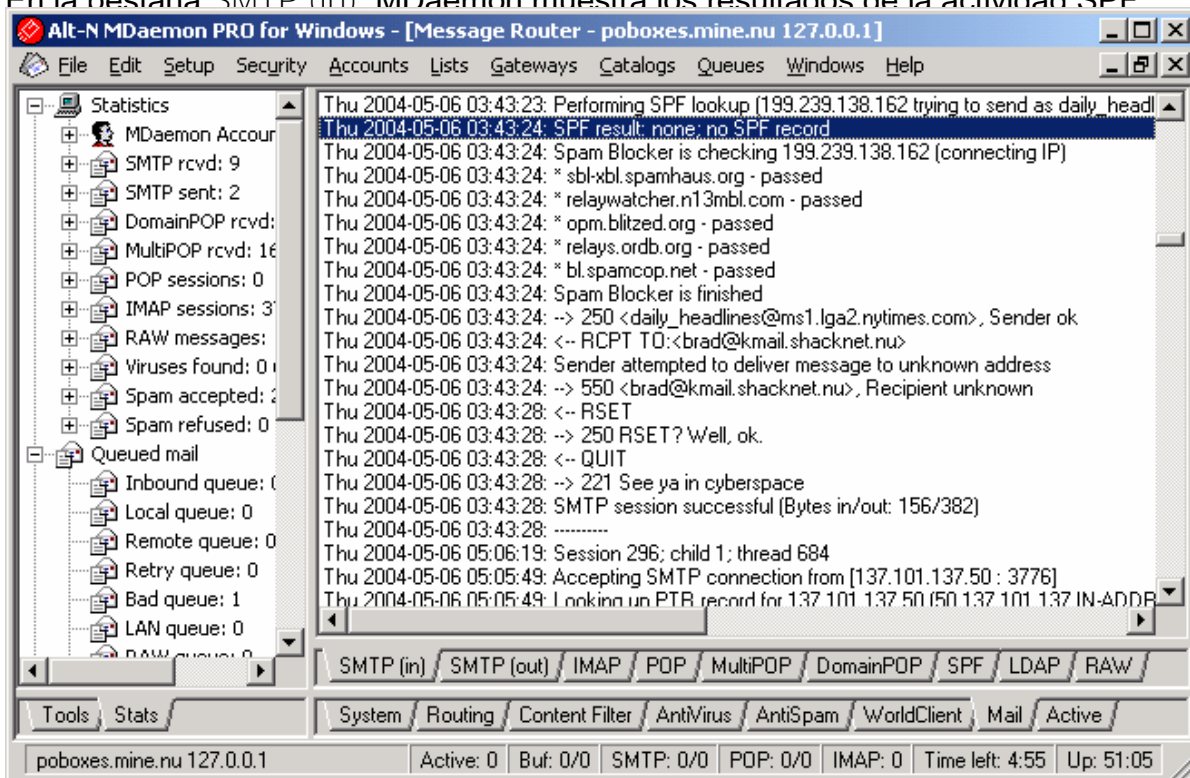
```
# SPF Cache File
#
# Note: Lines beginning with # are comments.
# Create entries of the form:
#
# Domain IP = <result> for [xx] more minutes.
# <result> = pass, fail, softfail, or neutral
#
# Examples:
#
# mail.domain.com 192.168.0.1 = pass for [10] more minutes.
# programming.domain.com 128.0.0.3 = fail for [60] more minutes.
```

Tracking SPF

Se puede hacer el seguimiento de la actividad SPF con la pestaña SMTP (In), la pestaña SPF y el archivo

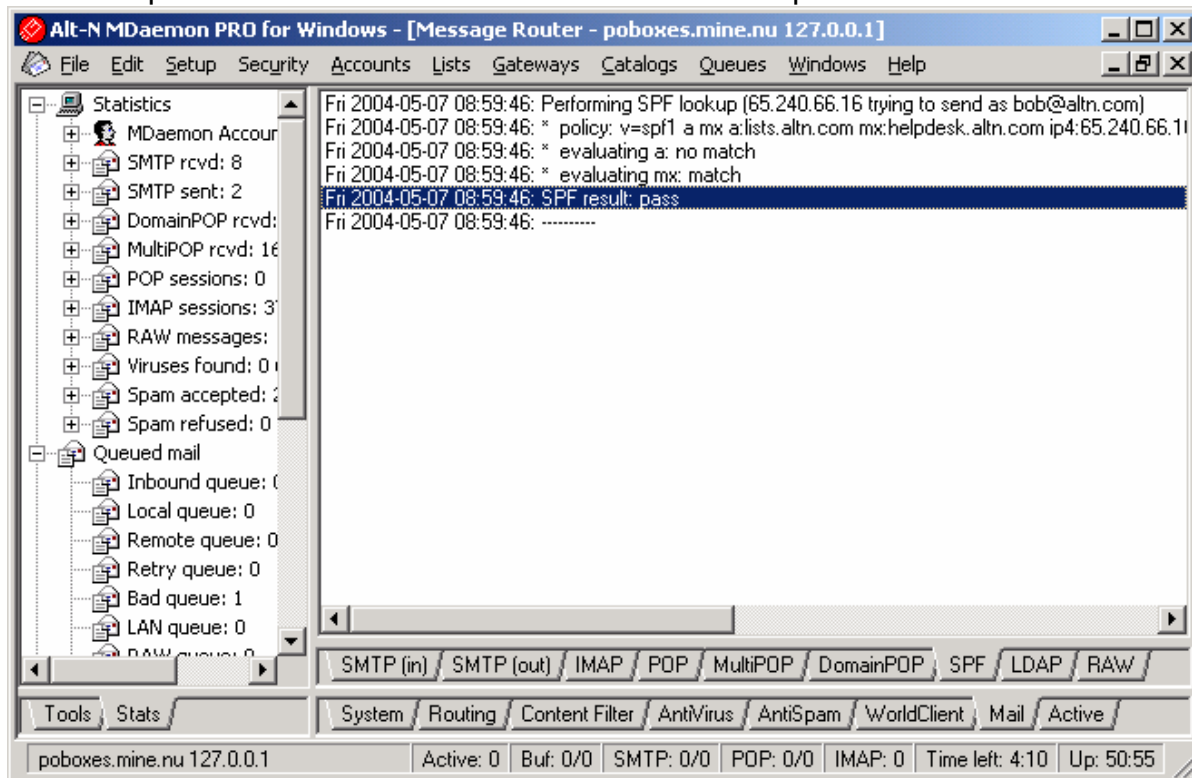
Pestaña SMTP (In)

En la pestaña SMTP (In) MDAemon muestra los resultados de la actividad SPF



Pestaña SPF

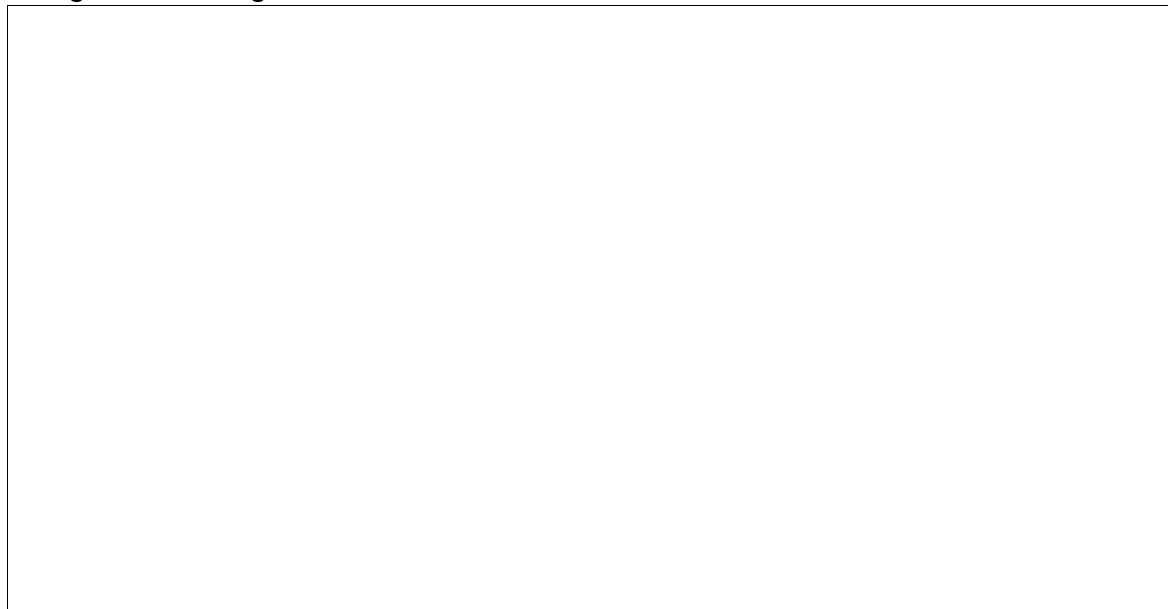
La pestaña SPF muestra los detalles de las búsquedas SPF:



Archivo MDAemon-SPF.log

MDAemon guarda un registro de la actividad SPF en el archivo

:



Configurar los registros de SPF

Información de la web de SPF

Para más información sobre la configuración de los registros SPF, visite la página web de SPF: <http://spf.pobox.com/>

El RFC se encuentra en: <http://spf.pobox.com/rfc.html>

También encontrará un asistente on-line que le ayudará a definir su registro SPF en: <http://spf.pobox.com/wizard.html>

Lo que debe saber

Para configurar registros SPF necesita conocer los contenidos de su registro DNS, las direcciones IP públicas de los equipos adicionales autorizados para enviar correo y los nombres de dominio de las IP que los usuarios que se desplazan pueden utilizar cuando estén fuera de la oficina.

Concretamente, debe determinar si su dominio envía e-mails desde:

- direcciones listadas en su registro DNS A.
- direcciones listadas en el registro A de su entrada DNS MX.
- direcciones listadas en el registro A de su entrada DNS PTR.
- otros equipos, incluyendo ordenadores personales que funcionen con servidores SMTP.
- direcciones de todas las IP.

Sesión de muestra con el Asistente

Este es un breve ejemplo que muestra como utilizar el asistente de registro SPF desde: <http://spf.pobox.com/wizard.html>

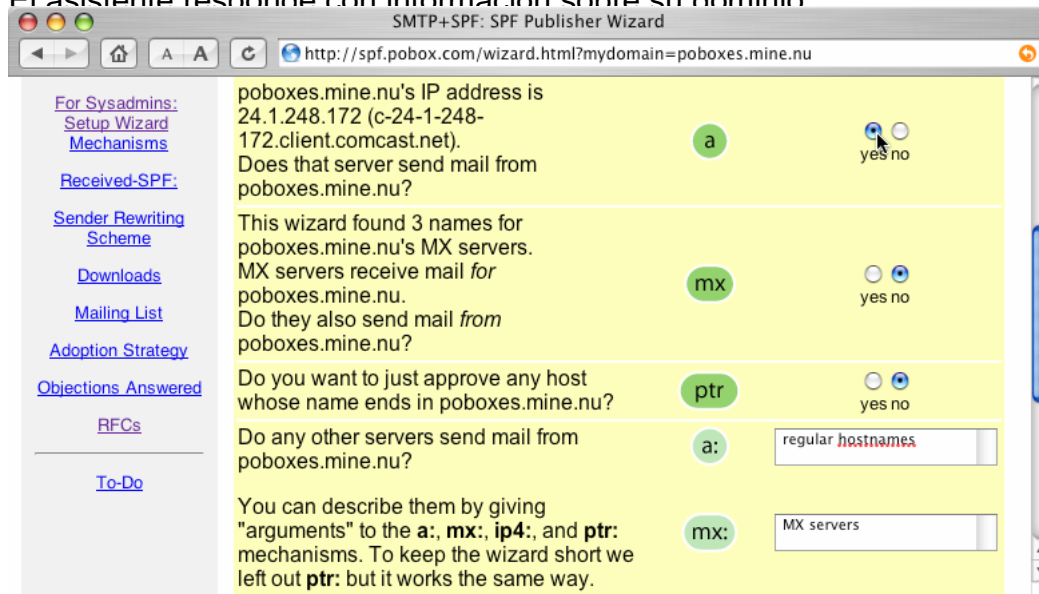
El asistente es muy útil para empezar a utilizar SPF. En muchos casos, puede crear el contenido completo de su registro SPF.

1. Ir a <http://spf.pobox.com/wizard.html>



2. Entre el *nombre de su dominio* y pulse el botón Empezar.

El asistente responde con información sobre su dominio



3. Vaya bajando por el asistente y entre la información necesaria. Le solicitará información como sus registros DNS *a* y *mx*.

A medida que Usted entra información, el asistente crea los contenidos de un registro SPF. Puede editar la información.

4. pulse el botón Explicar para visualizar los detalles de su registro.

5. Puede utilizar la cadena resultante como contenido de su registro SPF. El asistente le aconseja que lo realice con algunos servidores DNS.