Cuál es la mejor estrategia anti-spam posible para aplicar en un servidor de mail?

Aplicable a un dominio con muchas cuentas corporativas. Los 5 niveles para la mejor solución

Hoy en día una buena solución para seguridad en emails tiene que estar en constante equilibrio, sabiendo que se trata de un sistema que tendrá como objetivo principal:

- **Asegurar que aquello que sirve, o sea los mensajes válidos enviados, lleguen a destino sin inconvenientes**
- **Asegurar que aquello que sirve, o sea los mensajes válidos a recibir, se reciban sin inconvenientes**
- **Asegurar que aquello que no sirve, o sea el "correo basura", sea filtrado en su totalidad**
- **Asegurar que aquello que crea daños como virus y malware, sea eliminado en su totalidad**

Planteada esta necesidad de base, en esta nota pasaremos a recorrer los 5 niveles en los cuales se aplican estos criterios a nivel más técnico, entendiendo que los niveles 1,2 y 3 funcionarán 100% con responsabilidad nuestra (del proveedor de la solución de servidor de emails), y que los niveles 4 y 5 tienen una alta participación del usuario final, o al menos un usuario administrador del grupo si se tratase de muchas cuentas. En estos 2 últimos niveles participamos guiando inicialmente al usuario administrador, de modo de que sepa siempre qué pasos seguir para mantener el sistema de anti-spam lo más perfecto que se pueda.

NIVEL 5: PC DEL USUARIO

Esto abarca todo lo correspondiente a la pc del usuario: Operación y filtros en ***Outlook***, Antivirus de pc que actue sobre emails, etc.

NIVEL 4: FILTROS EN PANEL DE CONTROL Y WEBMAIL

Cuando entregamos servidores de email a clientes, una pieza clave será el panel de autogestión. Un usuario administrador podrá crear filtros a modo general, que permita aplicar un único criterio a todas las cuentas a la vez, como el caso de bloquear un dominio. Tambíen cada usuario podría aplicar lo mismo en su ***Webmail*** personal.

NIVEL 3: ANTIVIRUS y ANTISPAMS DEL PANEL

Este nivel comprende el software de seguridad que suele estar provisto junto al panel de autogestión del cloud server o dedicado. Como antivirus y detección de malware uno muy popular es ***ClamAV***. Para el caso de protección de emails, debería estar presente un componente como ***Amavis***. Y para anti-spam ***SpamAssasin***.

NIVEL 2: FIREWALLS

Todo servidor de email se econtrará en un entorno, de acuerdo a su sistema operativo, que permita aplicar bloqueos en la conectividad para su seguridad. En nuestro caso consideramos que debería haber 2 firewalls trabajando: uno a modo general (ejemplo ***CSF Firewall***), y uno con más ajustes para email como el caso de ***fail2ban***.

NIVEL 1: SERVIDOR DE EMAIL

Este nivel comprende las configuraciones aplicadas directamente sobre el servidor de email. En nuestro caso, en mail servers establecidos como ***Postfix***, ***Exim***, ***MailOne*** y ***Exchange*** solemos configurar la primera barrrera de seguridad siempre teniendo en cuenta que no debe perjudicarse a mensajes que sí deben recibirse.

En este cuadro se resumen los 5 niveles para poder aplicar lo que consideramos la emjor estrategia posible de anti-spam.

Cualquiera de los programas, servidores y plataformas de mailing que ofrecemos en **webmatter** permiten aplicar y revisar toda esta información en detalle, y tener configurado el SERVIDOR DE EMAIL de acuerdo a lo necesario para asegurar lo recien mencionado. Consúltenos para así obtener información actualizada sobre nuestros planes:

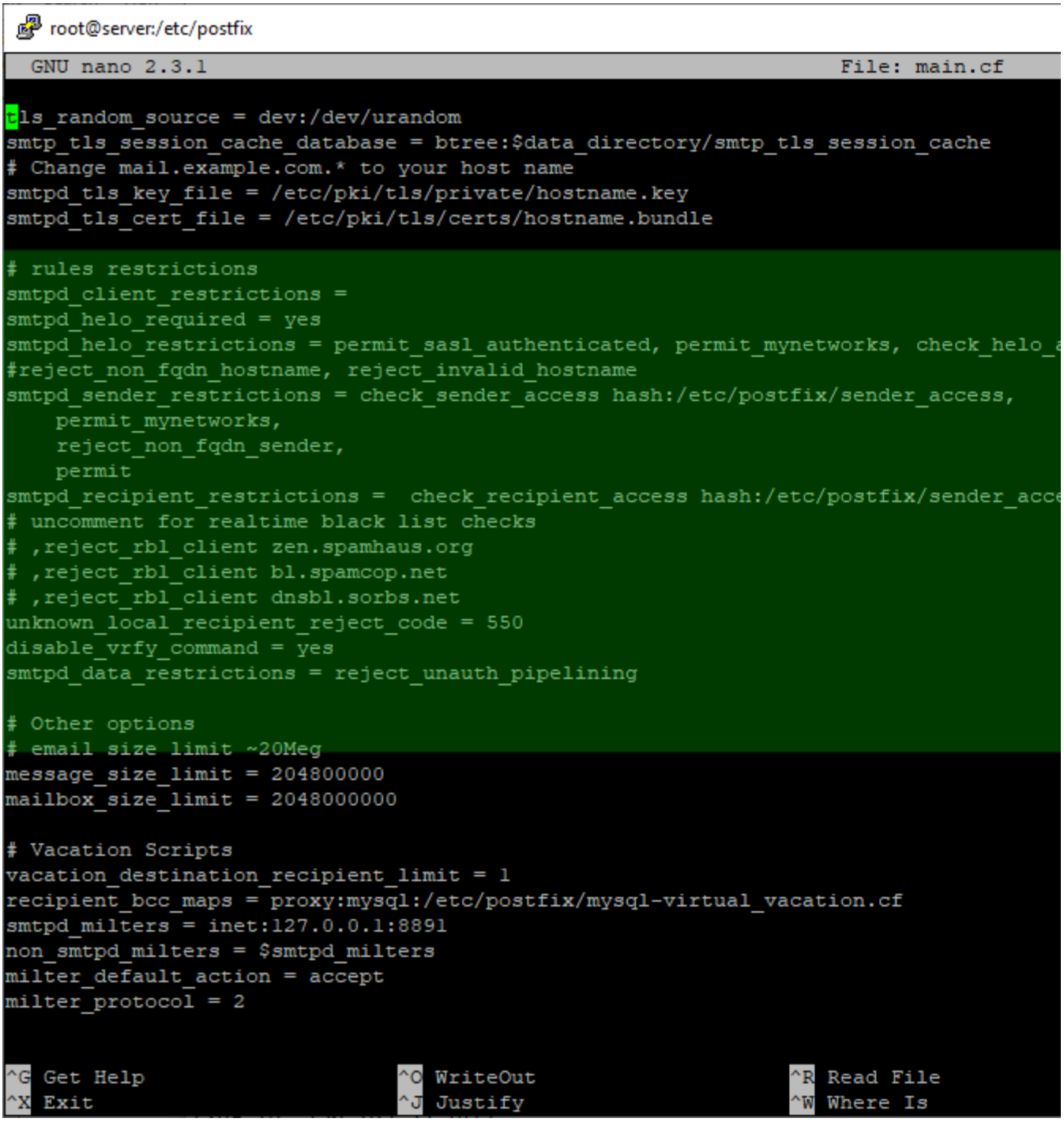
Chat	Teléfono	WhatsApp
Botón de CHAT ubicado abajo a la izquierda	**5411 47982212** (lun/vie 10/19 hs)	**54911 54594979** (lun/vie 10/19 hs)

A CONTINUACIÓN DESARROLLAMOS EN DETALLE LOS 5 NIVELES

NIVEL 1: SERVIDOR DE EMAIL

Este nivel comprende las configuraciones aplicadas directamente sobre el servidor de email. En nuestro caso, en mail servers establecidos como ***Postfix***, ***Exim***, ***MailOne*** y ***Exchange*** solemos configurar la primera barrrera de seguridad siempre teniendo en cuenta que no debe perjudicarse a mensajes que sí deben recibirse. Hay restricciones y reglas generales que siempre es bueno aplicarlas en esta instancia, para nunca poner en riesgo innecesariamente la seguridad del servidor. Por ejemplo mediante estas configuraciones se asegura que nunca podría salir un email con otro dominio desde el propio servidor, que siempre se recibiran mensajes de dominios reales, que sólo pueden salir emails autenticados con contraseña, que solo se aceptarán mensajes de dominios que no esten en listas negras como *Spamhaus*, etc, etc. Estas configuraciones de primer grado ahorrarán trabajo a los niveles restantes.

A continuación se muestra a modo ilustrativo una sección de la configuración del servidor ***Postfix***:



Es también en este nivel en el cual se aplican filtrados generales cuando se detecte un comportamiento inadecuado de emails que ingresan. Por ejemplo, supongamos que muy seguido se recibiera correo basura, todo proveniente de dominios de un país puntual determinado, en estas mismas configuraciones se podría aplicar el rechazo instantaneo de cualquier email que contenga el identificador de dominio del país en cuestión, por ejemplo .mx , .py, .ru, .uk, .de, etc etc. Como este tipo de medidas son muy abarcativas, son aplicables sólo cuando se sabe que no se pone en riesgo a mensajes que sí se desearan recibir en el futuro de parte de los usuarios.

NIVEL 2: FIREWALLS

Un firewall, como por ejemplo ***CSF Firewall***, es un software diseñado para proteger un sistema informático al filtrar el tráfico de red y bloquear el acceso no autorizado. Cuando un paquete de datos intenta entrar o salir del sistema, el firewall lo analiza para determinar si debe permitir o bloquear el tráfico.

El funcionamiento del firewall CSF comienza con su configuración en la cual se definen las reglas que se aplicarán al tráfico de red. Estas reglas pueden especificar qué puertos están abiertos para permitir el acceso a determinadas aplicaciones, restringir el acceso a direcciones IP específicas o bloquear ciertos tipos de tráfico.

Cuando se recibe un paquete de datos, el firewall lo examina en función de las reglas de filtrado configuradas. Si el paquete coincide con una regla permitida, se permite el acceso y el paquete se envía al destino correspondiente. Si el paquete no coincide con ninguna regla permitida, el firewall puede bloquearlo o permitirlo temporalmente hasta que se determine si es seguro o no.

El firewall también incluye otras características útiles, como la protección contra ataques de fuerza bruta (como ataques de diccionario de contraseñas) y la capacidad de enviar alertas por correo electrónico cuando se detectan actividades sospechosas en el servidor.

En resumen, el funcionamiento de un firewall como CSF se basa en la configuración de reglas que permiten o bloquean el tráfico de Internet entrante y saliente. Con una configuración adecuada, un firewall puede proporcionar una capa importante de seguridad para proteger un servidor contra ataques en línea.

En nuestras soluciones además de incluir el CSF FIREWALL, agregamos el software ***fail2ban*** que como firewall resulta indispensable por trabajar especificamente junto a sistemas de email como el caso de Postfix y otros, detectando al instante cualquier actividad sospechosa: por ejemplo cuando un virus de email reusa la cuenta de un usuario para enviar miles de correos basura, es a traves de fail2ban que esa acción puede detectarse y bloquearse.

NIVEL 3: ANTIVIRUS y ANTISPAMS DEL PANEL

Junto con el crecimiento de servidores dedicados, vps y cloud en internet, se popularizaron varios paneles para autogestionarlos, como el caso de WHM, cPanel, CWP, Virtualmin, DirectAdmin, etc.

Estos paneles hoy en día ya vienen provistos de buen software para anti-virus y anti-spam, por eso sugerimos que siempre estos componentes sean tenidos en cuenta, con la especial aclaración de que no deberían pasarse más de lo necesario en las acciones de filtrado y

bloqueo (al principio nos sucedía que se aplicaban filtros de más, como por ejemplo al considerar blacklists de poca relavancia para no dejar llegar determinados emails)

A modo de ejemplo repasaremos 3 componentes de importancia:

- **ClamAV (antivirus)**

ClamAV es un software antivirus de código abierto y gratuito, diseñado para detectar y eliminar virus, malware, troyanos y otros tipos de software malicioso en sistemas operativos Windows, Linux, macOS y otros.

ClamAV utiliza una combinación de técnicas de detección de virus, incluyendo análisis de firmas, análisis heurístico y detección de patrones de comportamiento, para identificar y neutralizar amenazas de seguridad en tiempo real. También cuenta con una base de datos de firmas de virus actualizable, que se mantiene constantemente actualizada para asegurarse de que el software esté equipado para detectar las últimas amenazas.

Además de la detección y eliminación de virus, ClamAV también es capaz de escanear archivos y directorios específicos, así como escanear correos electrónicos entrantes y salientes en busca de archivos adjuntos maliciosos. También es compatible con la integración de correo electrónico, lo que permite a los administradores de sistemas proteger a los usuarios de los ataques de phishing y spam.

En resumen, ClamAV es una herramienta de seguridad esencial para cualquier persona o empresa que desee proteger sus sistemas y datos de amenazas de seguridad en línea.

- **Amavis (anti-spam)**

Amavis es un software antivirus y antispam de código abierto que se utiliza para proteger los servidores de correo electrónico de virus y correo no deseado. Es compatible con una amplia gama de servidores de correo electrónico, como Postfix, Sendmail y Exim, y se ejecuta en sistemas operativos basados en Unix, como Linux y FreeBSD.

Amavis funciona como un filtro de correo electrónico, analizando cada mensaje entrante y saliente en busca de virus y spam utilizando múltiples técnicas de detección, como análisis de firmas, análisis heurístico y análisis de reputación de remitentes. También puede integrarse con múltiples motores de antivirus y antispam, lo que aumenta su capacidad para detectar y eliminar amenazas de seguridad.

Además, Amavis ofrece una serie de características de seguridad adicionales, como el soporte para listas negras y blancas de remitentes y destinatarios, autenticación de correo electrónico basada en políticas, filtrado de archivos adjuntos y cifrado de correo electrónico.

En resumen, Amavis es una herramienta de seguridad esencial para cualquier empresa que gestione grandes volúmenes de correo electrónico y desee protegerse contra virus, malware y spam. Con su amplia gama de características de seguridad y compatibilidad con múltiples servidores de correo electrónico, Amavis es una opción popular para administradores de sistemas y proveedores de servicios de correo electrónico.

- **SpamAssasin (anti-spam)**

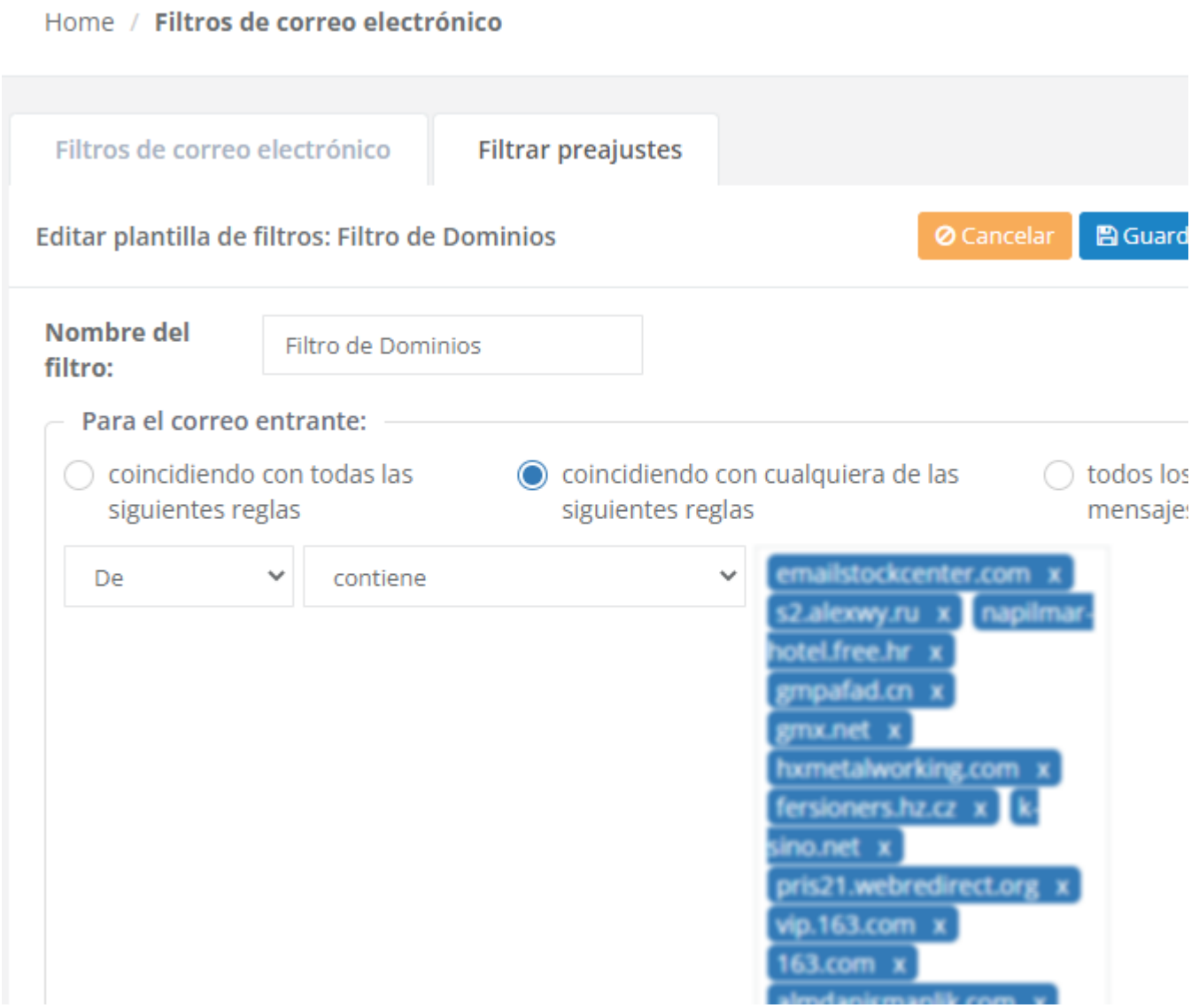
Spam Assassin es un software de código abierto diseñado para detectar y filtrar correos electrónicos no solicitados o no deseados, comúnmente conocidos como spam. Utiliza una combinación de técnicas como listas negras, listas blancas, filtrado bayesiano y coincidencia de patrones para analizar el contenido y encabezado de los correos electrónicos entrantes y asignar un puntaje de spam en función de la probabilidad de que sea spam.

Spam Assassin puede ser instalado en servidores de correo electrónico o utilizado como un filtro de correo electrónico independiente. Se integra con varios clientes y plataformas de correo electrónico, incluyendo Microsoft Outlook, Mozilla Thunderbird y Gmail.

Cuando se recibe un correo electrónico, Spam Assassin asigna un puntaje de spam al mismo. Si el puntaje supera cierto umbral, el correo electrónico se clasifica como spam y se puede filtrar, marcar, mover a la carpeta de spam o eliminar automáticamente según la configuración del usuario. El objetivo principal de Spam Assassin es reducir la cantidad de correo no deseado que los usuarios reciben en sus bandejas de entrada.

NIVEL 4: FILTROS EN PANEL DE CONTROL Y WEBMAIL

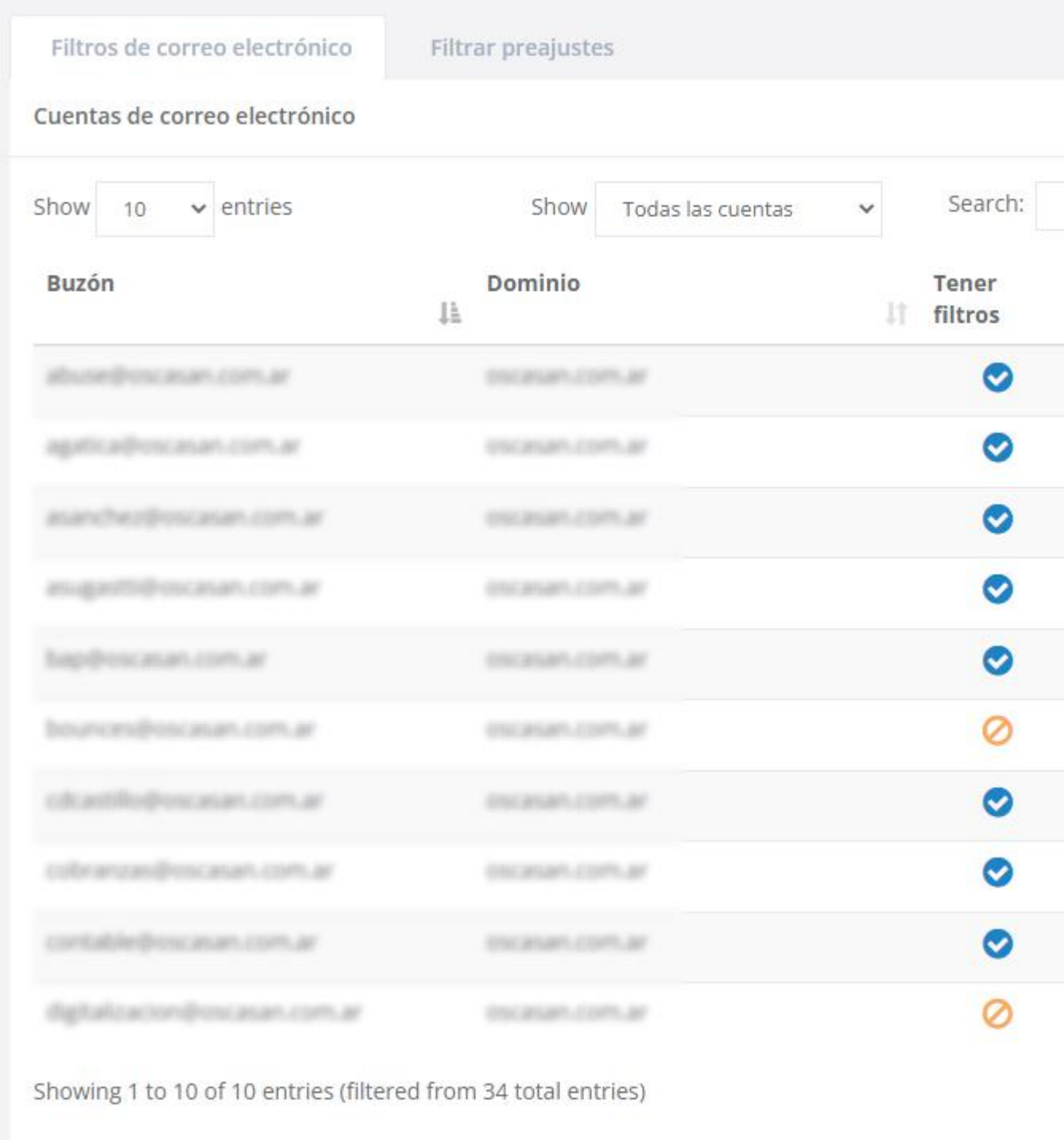
En este caso se consideraran los filtros basados en reglas, las cuales son aplicadas por los propios usuarios, o un usuario administrador, a partir de detectar casos de spam en al menos 1 casilla del dominio. Estos filtros utilizan un conjunto de reglas predefinidas para evaluar los mensajes de correo electrónico entrantes. Si un mensaje cumple con ciertas reglas específicas, se marca como spam y se eliminará automáticamente.



Mediante los filtros se pueden aplicar reglas, por ejemplo en este caso se listan dominios de emails que se deben rechazar y eliminar al recibirse

Existen 2 maneras de aplicar este tipo de filtros:

- En un panel central que nuclea a todas las cuentas. En este caso los filtros son creados y asignados por un administrador en el panel del servidor, normalmente en la nube.
- Cada usuario cree sus propios filtros, en el caso de nuestros clientes, esta opción suele realizarse en el webmail ***Roundcube***



Una vez creados los filtros, el administrador decide a qué usuario le asigna un determinado grupo de filtros creados

NIVEL 5: PC DEL USUARIO

Para un usuario con cuenta de dominio de empresa, la forma más habitual de operar sus correos hoy en día sería con programas de pc como ***Outlook*** y/o ***Mozilla Thunderbird*** Estas computadoras con programas "cliente" de email funcionando vendrían a conformar el último eslabón de la cadena que veníamos describiendo. Por lo cual teniendo en cuenta que se ha aplicado lo descripto en los niveles 1 a 4, la cantidad de correo basura a recibir a esta altura debería ser mínima, casi inexistente. La acción más comun ante cualquier caso de spam aislado que se detecte, debería ser abrir el menú con el botón derecho del mouse y enviar ese mensaje a la carpeta de "No deseado", de modo de que un próximo caso ese remitente no vuelva a interferir en la bandeja de entrada. Tambien debería marcarse la opción "bloquear remitente", buscando que nunca más esa dirección origen intente volver a llegar.

Pero esto no termina aquí: cada pc de usuario, si fuera víctima de un virus o ataque mal-ware, podría ser una amenaza que termine afectando al mismísimo servidor de email. La forma más habitual y dañina de virus en estos casos, es aquel que reusa la cuenta del usuario, usurpando los datos existentes en el programa cliente (email, servidor, puerto y contraseña). Una vez que se apodera de dicha información, los virus de pc suelen enviar correo masivo spam con la mismísima cuenta de la persona que opera esa máquina. Esta situación obliga a siempre estar pendientes de no tener virus en la pc y pasar periódicamente programas antivirus de pc que esten bien actualizados.

Cualquiera de los programas, servidores y plataformas de mailing que ofrecemos en **webmatter** permiten aplicar y revisar toda esta información en detalle, y tener configurado el SERVIDOR DE EMAIL de acuerdo a lo necesario para asegurar lo recien mencionado.
Consúltenos para así obtener información actualizada sobre nuestros planes:

Chat	Teléfono	WhatsApp
Botón de CHAT ubicado abajo a la izquierda en https://web-matter.com.ar	**5411 47982212** (lun/vie 10/19 hs)	**54911 54594979** (lun/vie 10/19 hs)