EBENEZER IT · GUÍAS PASO A PASO

GUÍA 09 · EPISODIOS 17 Y 18

Webmail, filtro de spam y protección del correo

Roundcube para leer el correo desde el navegador, tu móvil y tu PC configurados, Rspamd para que el spam y el phishing vayan solos a la carpeta Spam (y aprenda de ti), y las protecciones que impiden que alguien use tu servidor para hacerse pasar por otro o adivinar contraseñas.

~3–4 horas
la primera vez, en dos sesiones

Requisito
Guía 08 terminada

Ubuntu 24.04 LTS
Roundcube · Rspamd · fail2ban

www.ebenezer.org.es · Alejandro Quevedo · Versión pública 1.0 · noviembre 2026

Índice

Antes de empezar

0 Qué vas a construir y valores de esta guía

Parte A · Webmail con Roundcube

Paso 01 Qué es Roundcube y dónde va

Paso 02 Instalarlo sin Apache

Paso 03 Configurar Roundcube

Paso 04 El sitio: mail.TU_DOMINIO, solo por la VPN

Paso 05 Primer acceso

Parte B · Tus programas de correo

Paso 06 Los datos de conexión

Paso 07 El móvil

Paso 08 El PC

Parte C · Filtro de spam con Rspamd

Paso 09 Cómo decide Rspamd qué es spam

Paso 10 Instalar Rspamd y Redis

Paso 11 Configuración básica

Paso 12 Un DNS propio para las listas negras

Paso 13 Conectarlo a Postfix

Paso 14 El spam, directo a la carpeta Spam

Paso 15 Que aprenda de ti

Paso 16 Probar el filtro

Parte D · Protección

Paso 17 Que nadie envíe con un nombre que no es suyo

Paso 18 fail2ban para el correo

Paso 19 Comprobación final e instantánea

Anexos

A Problemas frecuentes

B Puertos y servicios al terminar esta guía

C Chuleta del filtro de spam

Cómo usar esta guía

Tienes aquí **todos los pasos y comandos**, en orden. La explicación de cada paso (el porqué de cada línea) está en el **vídeo del episodio**.

Para copiar los comandos sin errores, usa la versión web: **https://www.ebenezer.org.es/guia-09-webmail-spam.html**. Al copiar desde un PDF se pueden romper los saltos de línea y las comillas.

ANTES DE EMPEZAR

Qué vas a construir

La Guía 08 terminó con el correo funcionando y un 10/10 en mail-tester: tus correos llegan bien. Esta guía se ocupa de lo que **recibes** y de cómo lo usas: leerlo desde cualquier sitio, que el spam no te llene la bandeja y que nadie abuse de tu servidor.

Pieza	Qué hace	Dónde vive
Roundcube	Webmail: leer y escribir correo desde el navegador	`https://mail.TU_DOMINIO`, solo desde la VPN
Rspamd	Puntúa cada correo que llega (SPF, DKIM, DMARC, listas negras, contenido, enlaces) y decide: entregar, marcar como spam o rechazar	Servicio del sistema, solo en `127.0.0.1`
Redis	La memoria de Rspamd: lo que aprende y sus estadísticas	Servicio del sistema, solo en `127.0.0.1`, máximo 128 MB
Unbound	Un DNS propio para que las listas negras respondan a Rspamd	Servicio del sistema, solo en `127.0.0.1:5335`
Sieve	Reglas de Dovecot: lo marcado como spam va a la carpeta Spam, y lo que mueves enseña a Rspamd	Dentro de Dovecot
fail2ban	Bloquea a quien prueba contraseñas contra el 587 y el 993	El de la Guía 01, con dos reglas nuevas

El recorrido de un correo que entra, al terminar

1. Llega por el 25. Postfix se lo pasa primero a **Rspamd**, que le pone una nota.
2. Con **15 puntos o más** se rechaza en la puerta: el remitente recibe el error, tú no ves nada.
3. Con **6 o más** se acepta, pero con la marca `X-Spam: Yes`.
4. OpenDKIM comprueba su firma, y Dovecot lo entrega. **Sieve** ve la marca y lo deja en la carpeta **Spam** en vez de en la bandeja de entrada.
5. Si algo se cuela o se equivoca, lo mueves tú, y Rspamd **aprende** de ello.

Valores de esta guía

Valor	Qué es
`TU_DOMINIO`	Tu dominio
`TU_BUZON`	Tu buzón (lo de antes de la @)
`TU_CORREO_EXTERNO`	Un correo tuyo de fuera, para las pruebas
`TU_PASS_BD_CORREO`	La contraseña del usuario de solo lectura de la base de datos (Guía 08, paso 6)

Valor	Qué es
`TU_TOKEN_PRO`	Tu token de Ubuntu Pro (paso 1, opcional)

Recordatorio

- Haz una instantánea en IONOS antes de empezar.
- Memoria: Rspamd, Redis y Unbound juntos necesitan unos 350 MB. Con el VPS del curso vas sobrado; en un servidor más justo, mira antes `free -h`.
- Bloques **verdes** en el servidor, **azules** en PowerShell de tu PC, **morados** son contenido de archivos, **ocres** son clics en un panel.

PARTE A

Webmail con Roundcube

Un webmail para leer y escribir correo desde el navegador, cerrado a la VPN como el resto de paneles. Corresponde al **episodio 17**.

Paso 1 Episodio 17

Qué es Roundcube y dónde va

Por qué: Roundcube es un programa de correo que funciona en el navegador.

Decisión	Por qué
En `https://mail.TU_DOMINIO`	Es el nombre que la gente espera para el correo, y ya tiene certificado (Guía 08)
Solo desde la VPN	Un webmail es lo más atacado de un servidor de correo: formularios de acceso, PHP, adjuntos. Tú y tu equipo usáis la VPN; para el día a día, el móvil y el PC van directos por IMAP y SMTP cifrados
Paquete de Ubuntu	Se actualiza con el sistema. Con Ubuntu Pro (gratis para uso personal) recibe además los parches de seguridad de Roundcube

Activa Ubuntu Pro

Roundcube está en el repositorio «universe»: sin Ubuntu Pro, sus parches de seguridad no llegan. Es gratis hasta 5 máquinas: `ubuntu.com/pro/dashboard` → copia tu token → `sudo pro attach TU_TOKEN_PRO`. Activa también **Livepatch**: parches del kernel sin reiniciar. El token no se comparte con nadie.

Comprueba antes de seguir

Sabes por qué el webmail va cerrado a la VPN y por qué tus programas de correo no lo necesitan.

Paso 2 Episodio 17

Instalarlo sin Apache

Por qué: el paquete de Roundcube puede arrastrar Apache como servidor web, que chocaría con Nginx por el puerto 80.

EN EL SERVIDOR

```
sudo apt install --no-install-recommends roundcube roundcube-mysql roundcube-plugins
```

- Antes de pulsar **S**, lee la lista de paquetes nuevos: **no** debe aparecer `apache2`. Si aparece, responde **n** y revisa que Nginx está instalado (Guía 02).
- **¿Configurar la base de datos con dbconfig-common?** → **Sí**. Crea una base de datos propia para Roundcube (contactos, ajustes de cada usuario) en tu MariaDB.

- **Contraseña de MySQL para roundcube** → déjala en blanco y pulsa Intro: genera una aleatoria y la guarda en su configuración. No la necesitarás.

Comprueba antes de seguir

`ls /var/lib/roundcube/public_html/index.php` existe y `dpkg -l apache2` responde que no está instalado.

Paso 3 Episodio 17

Configurar Roundcube

Por qué: el paquete deja su configuración en `/etc/roundcube/config.inc.php`.

EN EL SERVIDOR

```
sudo cp -a /etc/roundcube/config.inc.php /etc/roundcube/config.inc.php.orig
sudo tee -a /etc/roundcube/config.inc.php > /dev/null <<'EOF'
// ---- Ebenezer IT (Guía 09): lo que va aquí manda sobre lo de arriba ----
$config['imap_host'] = 'ssl://mail.TU_DOMINIO:993';
$config['smtp_host'] = 'tls://mail.TU_DOMINIO:587';
$config['smtp_user'] = '%u';
$config['smtp_pass'] = '%p';
$config['product_name'] = 'Correo TU_DOMINIO';
$config['skin'] = 'elastic';
$config['plugins'] = ['archive', 'zipdownload', 'markasjunk'];
$config['session_lifetime'] = 30;
$config['ip_check'] = true;
$config['login_rate_limit'] = 3;
$config['support_url'] = '';
EOF
sudo php -l /etc/roundcube/config.inc.php
```

Comprueba antes de seguir

`php -l` responde `No syntax errors detected`.

Paso 4 Episodio 17

El sitio: mail.TU_DOMINIO, solo por la VPN

Por qué: en la Guía 08, `mail.TU_DOMINIO` solo tenía el puerto 80 para pedir el certificado.

EN EL SERVIDOR

```
sudo tee /etc/nginx/sites-available/mail.TU_DOMINIO > /dev/null <<'EOF'
# HTTP: Let's Encrypt y redirección a HTTPS
server {
    listen 80;
    listen [::]:80;
    server_name mail.TU_DOMINIO;

    location ^~ /.well-known/acme-challenge/ {
        root /var/www/letsencrypt;
    }

    location / {
        return 301 https://$host$request_uri;
    }
}

# HTTPS: Roundcube, solo desde la VPN
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name mail.TU_DOMINIO;

    ssl_certificate     /etc/letsencrypt/live/mail.TU_DOMINIO/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/mail.TU_DOMINIO/privkey.pem;
    include snippets/tls.conf;
    include snippets/solo-vpn.conf;

    # Quien no está en la VPN no ve un error: va a tu web
    error_page 403 = @fuera;
    location @fuera {
        return 302 https://www.TU_DOMINIO/;
    }

    add_header Strict-Transport-Security "max-age=86400" always;
    add_header X-Content-Type-Options "nosniff" always;
    add_header Referrer-Policy "strict-origin-when-cross-origin" always;
    add_header X-Frame-Options "SAMEORIGIN" always;

    root /var/lib/roundcube/public_html;
    index index.php;

    location / {
        try_files $uri $uri/ /index.php?$args;
    }

    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.3-fpm.sock;
    }

    location ~ /\. {
        deny all;
    }

    access_log /var/log/nginx/mail.access.log;
```

```
    error_log  /var/log/nginx/mail.error.log;
}
EOF
sudo nginx -t && sudo systemctl reload nginx
```

Comprueba antes de seguir

- Con la VPN: `https://mail.TU_DOMINIO` muestra el acceso de Roundcube.
- Sin la VPN: te lleva a `https://www.TU_DOMINIO`.

Paso 5 Episodio 17

Primer acceso

Por qué: entra con tu buzón y deja visibles las carpetas que usaremos.

1. Con la VPN, en `https://mail.TU_DOMINIO`: usuario `TU_BUZON@TU_DOMINIO` (la dirección completa) y su contraseña.
2. **Configuración** → **Carpetas**: comprueba que **Junk**, **Sent**, **Drafts** y **Trash** están activadas (suscritas). Roundcube solo muestra las carpetas suscritas.
3. **Configuración** → **Preferencias** → **Carpetas especiales**: Borradores = Drafts, Enviados = Sent, Spam = Junk, Papelera = Trash.
4. Envía un correo a TU_CORREO_EXTERNO y responde desde allí.

Comprueba antes de seguir

Lees, envías y recibes desde Roundcube, y las cuatro carpetas especiales están en su sitio.

PARTE B

Tus programas de correo

El móvil y el PC se conectan directamente a Dovecot y a Postfix, siempre cifrado. No necesitan la VPN. Corresponde al **episodio 17**.

Paso 6 Episodio 17

Los datos de conexión

Por qué: son los mismos para cualquier programa.

	Recibir (IMAP)	Enviar (SMTP)
Servidor	`mail.TU_DOMINIO`	`mail.TU_DOMINIO`
Puerto	**993**	**587**
Seguridad	**SSL/TLS**	**STARTTLS**
Usuario	`TU_BUZON@TU_DOMINIO` (completo)	El mismo
Contraseña	La del buzón	La misma
Autenticación	Contraseña normal	Contraseña normal

Si un programa propone otra cosa

Algunos programas «adivinan» y proponen el 143, el 110 o el 465, o «sin cifrado». No los aceptes: en tu servidor esos puertos están cerrados a propósito. Si un programa no conecta, casi siempre es por esto.

Comprueba antes de seguir

Tienes la tabla a mano para los pasos 7 y 8.

Paso 7 Episodio 17

El móvil

Por qué: cualquier app de correo con cuenta IMAP sirve.

App	Dónde está la configuración manual
Gmail (Android)	Añadir otra cuenta → **Otra** → escribe tu dirección → **Configuración manual** → **Personal (IMAP)**
Correo (iPhone)	Ajustes → Mail → Cuentas → Añadir cuenta → **Otra** → Añadir cuenta de correo → **IMAP**
K-9 Mail / Thunderbird (Android)	Añadir cuenta → tu dirección → **Configuración manual**

- Rellena con los datos del paso 6.

- Cuando la cuenta esté creada, mira las carpetas: la carpeta **Junk** puede aparecer como «Spam» o «Correo no deseado». Es la misma.
- Prueba: envía un correo desde el móvil a `TU_CORREO_EXTERNO` y comprueba que aparece en **Enviados** también en Roundcube (las dos ven el mismo buzón).

Mover a Spam desde el móvil también enseña a Rspamd

El aprendizaje del paso 15 funciona con cualquier programa que mueva correos por IMAP: Roundcube, el móvil o el PC.

Comprueba antes de seguir

El móvil recibe y envía, y lo enviado se ve también en Roundcube.

Paso 8 Episodio 17

El PC

Por qué: Thunderbird (gratuito) es el más sencillo con un servidor propio: suele detectar la configuración solo, pero conviene revisarla.

1. En Thunderbird: **Archivo** → **Nueva** → **Cuenta de correo existente**: tu nombre, tu dirección y tu contraseña.
2. Pulsa **Configurar manualmente** y comprueba que coincide con el paso 6 (993 SSL/TLS y 587 STARTTLS, usuario con la dirección completa).
3. **Hecho**. Si pregunta por una excepción de seguridad o por el certificado, **para**: tu certificado es de Let's Encrypt y es válido; si avisa, el nombre del servidor está mal escrito.

¿Y Outlook?

El Outlook nuevo de Windows sincroniza las cuentas IMAP a través de los servidores de Microsoft: tu contraseña y tus correos pasan por ellos. Funciona, pero si buscas que tu correo sea solo tuyo, Thunderbird lo trabaja directamente desde tu PC.

Comprueba antes de seguir

El PC recibe y envía con los datos del paso 6.

PARTE C

Filtro de spam con Rspamd

Hasta ahora, todo correo dirigido a un buzón que existe se entrega tal cual. Montamos Rspamd para que el spam y el *phishing* (como las facturas falsas) se queden fuera o vayan a la carpeta Spam, y para que aprenda de lo que tú corriges. Corresponde al **episodio 18**.

Paso 9 Episodio 18

Cómo decide Rspamd qué es spam

Por qué: Rspamd no tiene una lista de «correos malos»: aplica cientos de reglas, cada una suma o resta puntos, y la suma decide.

Ejemplo de regla	Puntos	Qué detecta
`R_SPF_ALLOW`, `R_DKIM_ALLOW`, `DMARC_POLICY_ALLOW`	Restan	El remitente está bien configurado y es quien dice ser
`DBL_SPAM`	+6,5	El dominio del remitente está en la lista negra de Spamhaus
`RCVD_UNAUTH_PBL`	+2	Lo envía una IP doméstica que no debería enviar correo directamente
`HFILTER_HOSTNAME_UNKNOWN`	+2,5	El servidor que lo envía no tiene un nombre válido
`R_DKIM_PERMFAIL`, `BROKEN_HEADERS`…	Suman	Firmas rotas, cabeceras mal formadas, fechas imposibles
`BAYES_SPAM`	Suma	Se parece a lo que tú has marcado como spam (paso 15)

Nota	Acción	Qué ves tú
Menos de 6	Ninguna	El correo en la bandeja de entrada
6 a 15	**add header**	El correo en la carpeta **Spam** (paso 14)
15 o más	**reject**	Nada: se rechaza en la entrada

Ningún filtro para el 100 %

Un *phishing* enviado desde una cuenta real robada pasa SPF y DKIM, porque técnicamente sí sale de ese dominio. Rspamd lo suele pillar por el contenido, los enlaces y las listas negras, pero la última barrera sigue siendo desconfiar de un remitente raro que te pide pagar o pulsar un enlace.

Comprueba antes de seguir

Sabes leer la línea `X-Spamd-Result` de un correo: la nota, el umbral y las reglas que han saltado.

Paso 10 Episodio 18

Instalar Rspamd y Redis

Por qué: los autores de Rspamd recomiendan su propio repositorio: el paquete de Ubuntu va muchas versiones por detrás.

EN EL SERVIDOR

```
sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://rspamd.com/apt-stable/gpg.key | sudo gpg --dearmor -o
/etc/apt/keyrings/rspamd.gpg
echo "deb [signed-by=/etc/apt/keyrings/rspamd.gpg] https://rspamd.com/apt-stable/ $(lsb_release
-cs) main" | sudo tee /etc/apt/sources.list.d/rspamd.list
sudo apt update
sudo apt install rspamd redis-server
printf '\n# Límite para Rspamd\nmaxmemory 128mb\nmaxmemory-policy allkeys-lru\n' | sudo tee -a
/etc/redis/redis.conf
sudo systemctl restart redis-server
redis-cli config get maxmemory
sudo ss -tlnp | grep -E ':(6379|11332|11333|11334) '
```

Comprueba antes de seguir

Redis (6379) y Rspamd (11332, 11333 y 11334) escuchan **solo** en `127.0.0.1`. Rspamd aún no recibe ningún correo: lo conectamos en el paso 13.

Paso 11 Episodio 18

Configuración básica

Por qué: Rspamd se ajusta con archivos pequeños en `/etc/rspamd/local.d/`: solo tus cambios, sin tocar los de fábrica, que así se actualizan sin conflictos.

EN EL SERVIDOR

```
echo 'servers = "127.0.0.1:6379";' | sudo tee /etc/rspamd/local.d/redis.conf

sudo tee /etc/rspamd/local.d/actions.conf > /dev/null <<'EOF'
# Qué hacer según la puntuación de cada correo
reject = 15;       # rechazar en la entrada: casi seguro spam
add_header = 6;    # entregar marcado como spam (irá a la carpeta Spam)
greylist = null;   # sin umbral de listas grises
EOF

echo 'enabled = false;' | sudo tee /etc/rspamd/local.d/greylist.conf

sudo tee /etc/rspamd/local.d/milter_headers.conf > /dev/null <<'EOF'
use = ["x-spamd-bar", "x-spam-level", "authentication-results"];
extended_spam_headers = true;
EOF

echo 'enabled = false;' | sudo tee /etc/rspamd/local.d/dkim_signing.conf
echo 'enabled = false;' | sudo tee /etc/rspamd/local.d/arc.conf
echo 'autolearn = true;' | sudo tee /etc/rspamd/local.d/classifier-bayes.conf

sudo rspamadm configtest && sudo systemctl restart rspamd
```

Comprueba antes de seguir

`rspamadm configtest` responde `syntax OK`.

Paso 12 Episodio 18

Un DNS propio para las listas negras

Por qué: las listas negras (Spamhaus, URIBL…) bloquean las consultas que llegan desde DNS públicos y compartidos, como el de tu proveedor: reciben millones.

EN EL SERVIDOR

```
sudo apt install unbound bind9-dnsutils
sudo systemctl disable --now unbound-resolvconf.service 2>/dev/null
sudo tee /etc/unbound/unbound.conf.d/rspamd.conf > /dev/null <<'EOF'
# DNS recursivo local, solo para Rspamd (listas negras)
server:
    interface: 127.0.0.1
    port: 5335
    access-control: 127.0.0.0/8 allow
    do-ip6: no
    hide-identity: yes
    hide-version: yes
    qname-minimisation: yes
    prefetch: yes
    num-threads: 1
    msg-cache-size: 16m
    rrset-cache-size: 32m
EOF
sudo unbound-checkconf && sudo systemctl restart unbound
grep nameserver /etc/resolv.conf
dig @127.0.0.1 -p 5335 2.0.0.127.multi.uribl.com +short
```

Ahora, que Rspamd use Unbound:

EN EL SERVIDOR

```
sudo tee /etc/rspamd/local.d/options.inc > /dev/null <<'EOF'
dns {
  nameserver = ["127.0.0.1:5335"];
}
EOF
sudo rspamadm configtest && sudo systemctl restart rspamd
```

Comprueba antes de seguir

`dig` por el 5335 responde `127.0.0.14` y `resolv.conf` sigue con `127.0.0.53`.

Paso 13 Episodio 18

Conectarlo a Postfix

Por qué: Rspamd se conecta a Postfix como un *milter* más, igual que OpenDKIM.

EN EL SERVIDOR

```
sudo postconf milter_protocol smtpd_milters
sudo postconf -e \
  'milter_protocol = 6' \
  'smtpd_milters = inet:127.0.0.1:11332, inet:127.0.0.1:8891'
sudo postfix check && sudo systemctl reload postfix
sudo postconf smtpd_milters non_smtpd_milters
```

Envíate un correo desde TU_CORREO_EXTERNO. En Roundcube, ábrelo → **Más** → **Ver código fuente**: debe tener la cabecera `X-Spamd-Result: default: False [-1.00 / 15.00]` (o parecida). Envía también uno desde tu buzón a fuera y comprueba que sigue llegando con **DKIM: PASS**.

Comprueba antes de seguir

Los correos que entran llevan `X-Spamd-Result`, los que salen siguen firmados, y `sudo grep -i milter /var/log/mail.log | tail` no muestra errores.

Paso 14 Episodio 18

El spam, directo a la carpeta Spam

Por qué: Rspamd marca, pero no mueve: un correo con 8 puntos llegaría a la bandeja de entrada con la marca puesta.

EN EL SERVIDOR

```
sudo apt install dovecot-sieve
sudo mkdir -p /etc/dovecot/sieve
sudo tee /etc/dovecot/sieve/spam-a-junk.sieve > /dev/null <<'EOF'
require ["fileinto", "mailbox"];

# Lo que Rspamd marca como spam va a la carpeta Junk (Spam)
if anyof (header :is "X-Spam" "Yes",
          header :is "X-Rspamd-Action" "add header") {
    fileinto :create "Junk";
    stop;
}
EOF
```

Las reglas se activan en el paso 15, junto con las de aprendizaje: van en el mismo archivo de configuración y hay que compilarlas después de activarlo.

Comprueba antes de seguir

Existe `/etc/dovecot/sieve/spam-a-junk.sieve`.

Paso 15 Episodio 18

Que aprenda de ti

Por qué: cuando muevas un correo a Spam, Rspamd lo aprenderá como spam; cuando lo saques, como correo bueno.

15.1 · Los dos programas que hablan con Rspamd

EN EL SERVIDOR

```
sudo tee /etc/dovecot/sieve/rspamd-aprender-spam.sh > /dev/null <<'EOF'
#!/bin/sh
exec /usr/bin/rspamc -h 127.0.0.1:11334 learn_spam
EOF
sudo tee /etc/dovecot/sieve/rspamd-aprender-ham.sh > /dev/null <<'EOF'
#!/bin/sh
exec /usr/bin/rspamc -h 127.0.0.1:11334 learn_ham
EOF
sudo chmod 755 /etc/dovecot/sieve/rspamd-aprender-*.sh
```

15.2 · Las dos reglas

EN EL SERVIDOR

```
sudo tee /etc/dovecot/sieve/aprender-spam.sieve > /dev/null <<'EOF'
require ["vnd.dovecot.pipe", "copy", "imapsieve"];
# Has metido este correo en Spam: Rspamd lo aprende como spam
pipe :copy "rspamd-aprender-spam.sh";
EOF
sudo tee /etc/dovecot/sieve/aprender-ham.sieve > /dev/null <<'EOF'
require ["vnd.dovecot.pipe", "copy", "imapsieve", "environment", "variables"];
# Has sacado este correo de Spam: Rspamd lo aprende como correo bueno
# (salvo si va a la Papelera: borrarlo no significa que sea bueno)
if environment :matches "imap.mailbox" "*" {
    set "destino" "${1}";
}
if string "${destino}" "Trash" {
    stop;
}
pipe :copy "rspamd-aprender-ham.sh";
EOF
```

15.3 · Activarlo todo en Dovecot y compilar

Créalo con `sudo nano /etc/dovecot/conf.d/99-sieve.conf`:

CONTENIDO DEL ARCHIVO · /ETC/DOVECOT/CONF.D/99-SIEVE.CONF

```
# Sieve al entregar (LMTP): el spam va a Junk
protocol lmtp {
  mail_plugins = $mail_plugins sieve
}

# Sieve al mover correos (IMAP): Rspamd aprende
protocol imap {
  mail_plugins = $mail_plugins imap_sieve
}

plugin {
  sieve = file:/var/mail/vhosts/%d/%n/sieve;active=/var/mail/vhosts/%d/%n/.dovecot.sieve
  sieve_before = /etc/dovecot/sieve/spam-a-junk.sieve

  sieve_plugins = sieve_imapsieve sieve_extprograms
  sieve_global_extensions = +vnd.dovecot.pipe +vnd.dovecot.environment
  sieve_pipe_bin_dir = /etc/dovecot/sieve

  # Al meter un correo en Junk: aprender como spam
  imapsieve_mailbox1_name = Junk
  imapsieve_mailbox1_causes = COPY
  imapsieve_mailbox1_before = file:/etc/dovecot/sieve/aprender-spam.sieve

  # Al sacarlo de Junk: aprender como correo bueno
  imapsieve_mailbox2_name = *
  imapsieve_mailbox2_from = Junk
  imapsieve_mailbox2_causes = COPY
  imapsieve_mailbox2_before = file:/etc/dovecot/sieve/aprender-ham.sieve
}
```

EN EL SERVIDOR

```
sudo doveconf -n > /dev/null && echo "configuracion correcta" && sudo systemctl reload dovecot
sudo sievec /etc/dovecot/sieve/spam-a-junk.sieve
sudo sievec /etc/dovecot/sieve/aprender-spam.sieve
sudo sievec /etc/dovecot/sieve/aprender-ham.sieve
ls /etc/dovecot/sieve/*.svbin
```

El aprendizaje tarda en notarse

El filtro bayesiano no empieza a puntuar hasta que ha aprendido unos 200 spams y 200 correos buenos. Mientras tanto, el resto de reglas funcionan desde el primer correo. Los primeros días, mueve tú lo que se cuele y saca de Spam lo que no lo sea.

Comprueba antes de seguir

`configuracion correcta` y existen los tres `.svbin`.

Paso 16 Episodio 18

Probar el filtro

Por qué: probamos las tres piezas por separado, de forma que el resultado no dependa de que hoy te llegue spam.

16.1 · Sieve: un correo marcado va a Junk

EN EL SERVIDOR

```
printf 'From: prueba@ejemplo.com\nTo: TU_BUZON@TU_DOMINIO\nSubject: prueba\nX-Spam:
Yes\n\nHola\n' > /tmp/marcado.eml
sudo sieve-test /etc/dovecot/sieve/spam-a-junk.sieve /tmp/marcado.eml
rm /tmp/marcado.eml
```

SALIDA ESPERADA

```
Performed actions:

 * store message in folder: Junk
```

16.2 · Rspamd: un correo de prueba que debe rechazar

Rspamd reconoce un texto de prueba estándar (GTUBE), pero lo trae desactivado para que nadie lo use contra tu filtro. Lo activamos un momento, probamos y lo apagamos.

EN EL SERVIDOR

```
sudo sed -i 's|^dns {|enable_test_patterns = true;\ndns {|' /etc/rspamd/local.d/options.inc
sudo rspamadm configtest && sudo systemctl restart rspamd
swaks --server mail.TU_DOMINIO --port 25 --from prueba@ejemplo.com --to TU_BUZON@TU_DOMINIO \
  --body 'XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X' | tail -n 4
sudo sed -i '/^enable_test_patterns = true;$/d' /etc/rspamd/local.d/options.inc
sudo rspamadm configtest && sudo systemctl restart rspamd
cat /etc/rspamd/local.d/options.inc
```

16.3 · El aprendizaje

1. En Roundcube, mueve un correo normal (un boletín, por ejemplo) de la Entrada a **Junk**.
2. Espera unos segundos y devuélvelo a la Entrada.

EN EL SERVIDOR

```
sudo grep -E "learned message as" /var/log/rspamd/rspamd.log | tail -n 2
rspamc -h 127.0.0.1:11334 stat | grep -E "learned"
```

SALIDA ESPERADA

```
... learned message as spam: ...
... learned message as ham: ...
```

Primero lo aprende como spam y, al sacarlo, deshace ese aprendizaje y lo aprende como bueno (`unlearn=true`). Si te equivocas al mover, se corrige solo.

Rspamd no aprende dos veces el mismo correo

Si repites la prueba con el mismo mensaje, el contador no sube: el registro dirá *already learned*. Usa cada vez un correo distinto.

Comprueba antes de seguir

- `sieve-test` → `store message in folder: Junk`.
- El GTUBE se rechaza con `554`, y el modo de prueba queda apagado.
- El registro muestra `learned message as spam` y `as ham`.

PARTE D

Protección

Dos últimas defensas: que un usuario de tu servidor no pueda enviar como otro, y que quien pruebe contraseñas acabe bloqueado. Corresponde al **episodio 18**.

Paso 17 Episodio 18

Que nadie envíe con un nombre que no es suyo

Por qué: ahora mismo, cualquiera con un buzón en tu servidor puede enviar por el 587 poniendo como remitente **otra** dirección, por ejemplo la de un compañero o `facturacion@TU_DOMINIO`.

EN EL SERVIDOR

```
sudo tee /etc/postfix/sql/remitentes.cf > /dev/null <<'EOF'
user = mailuser
password = TU_PASS_BD_CORREO
hosts = 127.0.0.1
dbname = mailserver
query = SELECT username FROM mailbox WHERE username='%s' AND active = 1 UNION SELECT goto FROM
alias WHERE address='%s' AND active = 1
EOF
sudo chown root:postfix /etc/postfix/sql/remitentes.cf
sudo chmod 640 /etc/postfix/sql/remitentes.cf
sudo postmap -q TU_BUZON@TU_DOMINIO mysql:/etc/postfix/sql/remitentes.cf

sudo postconf -e 'smtpd_sender_login_maps = mysql:/etc/postfix/sql/remitentes.cf'
sudo postconf -P
"submission/inet/smtpd_sender_restrictions=reject_sender_login_mismatch,permit_sasl_authenticat
ed,reject"
sudo postfix check && sudo systemctl reload postfix
```

EN EL SERVIDOR

```
swaks --server mail.TU_DOMINIO --port 587 --tls --auth LOGIN --auth-user TU_BUZON@TU_DOMINIO \
  --from director@TU_DOMINIO --to TU_CORREO_EXTERNO | tail -n 4
```

SALIDA ESPERADA

```
<** 553 5.7.1 <director@TU_DOMINIO>: Sender address rejected: not owned by user
TU_BUZON@TU_DOMINIO
```

Comprueba antes de seguir

Enviar como otra dirección se rechaza con `553 ... not owned by user`, y enviar como tu buzón sigue funcionando.

Paso 18 Episodio 18

fail2ban para el correo

Por qué: el 587 y el 993 están abiertos a Internet y piden contraseña: recibirán intentos de adivinarlas a diario.

EN EL SERVIDOR

```
sudo tee /etc/fail2ban/jail.d/correo.local > /dev/null <<'EOF'
[postfix-sasl]
enabled  = true
filter   = postfix[mode=auth]
port     = smtp,submission
logpath  = /var/log/mail.log
maxretry = 5
findtime = 10m
bantime  = 1h

[dovecot]
enabled  = true
port     = imaps,submission
logpath  = /var/log/mail.log
maxretry = 5
findtime = 10m
bantime  = 1h
EOF
sudo fail2ban-client -t && sudo systemctl reload fail2ban
sudo fail2ban-client status
```

¿Y Roundcube?
Roundcube está cerrado a la VPN, así que no necesita su propia regla. Si algún día lo abres a Internet, añade la jaula `[roundcube-auth]` con `logpath = /var/log/roundcube/errors.log`.

Comprueba antes de seguir
`fail2ban-client status` muestra, además de `sshd`, las jaulas `postfix-sasl` y `dovecot`.

Paso 19 Episodio 18

Comprobación final e instantánea

Por qué: repaso de todo, un reinicio y la instantánea que cierra la temporada del correo.

EN EL SERVIDOR

```
for s in postfix dovecot opendkim rspamd redis-server unbound fail2ban php8.3-fpm; do printf
"%-14s %s\n" $s $(systemctl is-active $s); done
sudo ss -tlnp | grep -E ':(25|587|993|5335|6379|8891|11332|11333|11334) '
sudo postconf smtpd_milters milter_protocol
sudo fail2ban-client status | grep "Jail list"
rspamc -h 127.0.0.1:11334 stat | grep -E "learned|scanned"
```

Comprobación	Resultado correcto
Servicios	Los ocho `active`
Puertos públicos	Solo **25**, **587** y **993**; todo lo demás (5335, 6379, 8891, 11332–11334) solo en `127.0.0.1`
Milters	`inet:127.0.0.1:11332, inet:127.0.0.1:8891` y `milter_protocol = 6`
fail2ban	`sshd`, `postfix-sasl` y `dovecot`
Webmail	Con VPN, Roundcube; sin VPN, tu web
Rspamd	`scanned` sube con cada correo que entra

Reinicia el servidor y, al volver, envíate un correo desde fuera: debe llegar con su `X-Spamd-Result`. Después, en IONOS, la instantánea `09-correo-completo`.

Si usas el script de chequeo diario de las descargas

Añade `rspamd redis-server unbound` a su lista `SERVICES`. Si uno de ellos se cae, el correo sigue entrando, pero sin filtrar: sin vigilancia, no te enterarías.

Dentro de dos semanas

Mira los correos que Rspamd puntuó entre 10 y 15 (`sudo grep -E "default: T \[1[0-4]\." /var/log/rspamd/rspamd.log`) y tu carpeta Spam. Si todo lo que ves es spam de verdad, baja `reject` a 13 en `actions.conf`.

Comprueba antes de seguir

Tu correo está completo: lo lees desde cualquier sitio, el spam se queda fuera o en su carpeta, aprende de ti, nadie puede enviar con un nombre ajeno y quien prueba contraseñas acaba bloqueado. Con esto termina la temporada del correo.

ANEXOS

Para cuando algo no sale

Tres registros cuentan casi todo: `/var/log/mail.log` (Postfix y Dovecot), `/var/log/rspamd/rspamd.log` (cada correo con su nota) y `/var/log/fail2ban.log`.

Anexo A · Problemas frecuentes

Lo que ves	Qué pasa	Qué hacer
Al instalar Roundcube aparece `apache2` en la lista	Falta un servidor web que «cuente» para el paquete	Responde **n**, comprueba `dpkg -l nginx` y repite con `--no-install-recommends`
Roundcube: *Connection to storage server failed*	No llega a Dovecot por el 993	`openssl s_client -connect mail.TU_DOMINIO:993 -quiet` desde el servidor; revisa `imap_host`
Roundcube: *SMTP Error (535): Authentication failed* al enviar	No usa tu usuario para el 587	Revisa `smtp_user = '%u'` y `smtp_pass = '%p'`
Los correos que entran no tienen `X-Spamd-Result`	Postfix no pasa por Rspamd	`postconf smtpd_milters milter_protocol`: debe incluir el 11332 y el protocolo 6. `systemctl status rspamd`
`URIBL_BLOCKED` en `X-Spamd-Result`	Rspamd no usa Unbound	Revisa `options.inc` y `dig @127.0.0.1 -p 5335 ...` (paso 12)
Correos legítimos con `451 4.7.1 Try again later`	El módulo de listas grises sigue activo	`local.d/greylist.conf` con `enabled = false;` y reinicia Rspamd
Lo marcado como spam sigue en la bandeja de entrada	Sieve no está activo en LMTP	`doveconf -n | grep -A2 "protocol lmtp"` debe incluir `sieve`; prueba con `sieve-test` (16.1)
`sievec`: *unknown Sieve capability vnd.dovecot.pipe*	Se compiló antes de activar la configuración	Recarga Dovecot con `99-sieve.conf` y vuelve a compilar
Mover a Spam no aprende nada	IMAPSieve no se lanza, o es un correo ya aprendido	Prueba con otro correo y mira `grep -i imapsieve /var/log/mail.log`
Un correo legítimo acaba en Spam	Alguna regla le suma de más	Sácalo de Spam (Rspamd aprende) y mira su `X-Spamd-Result` para ver qué reglas saltaron
`553 ... not owned by user` enviando como un alias tuyo	El alias no entrega a tu buzón	En PostfixAdmin, que el alias tenga tu buzón como destino

Anexo B · Puertos y servicios al terminar esta guía

Puerto	Servicio	Accesible desde
25 / 587 / 993	Postfix y Dovecot (Guía 08)	Todo Internet; 587 y 993 vigilados por fail2ban
443 → `mail.TU_DOMINIO`	Roundcube	Solo la VPN (los demás van a tu web)
127.0.0.1:11332	Rspamd: milter para Postfix	Solo el servidor
127.0.0.1:11333 / 11334	Rspamd: trabajadores y *controller* (aprendizaje)	Solo el servidor
127.0.0.1:6379	Redis	Solo el servidor
127.0.0.1:5335	Unbound	Solo el servidor

No se abre ningún puerto nuevo en IONOS ni en UFW.

Anexo C · Chuleta del filtro de spam

Para...	Cómo
Ver la nota de un correo	Roundcube → Más → Ver código fuente → `X-Spamd-Result`
Ver las últimas decisiones de Rspamd	`sudo tail -n 20 /var/log/rspamd/rspamd.log`
Puntuar un correo guardado	`sudo cat archivo-del-correo | rspamc` (los correos están en `/var/mail/vhosts/dominio/usuario/cur/` ; nunca los `dovecot.*`)
Estadísticas y aprendidos	`rspamc -h 127.0.0.1:11334 stat`
Enseñar un correo a mano	`sudo cat archivo | rspamc -h 127.0.0.1:11334 learn_spam` (o `learn_ham`)
Cambiar los umbrales	`/etc/rspamd/local.d/actions.conf` → `sudo rspamadm configtest && sudo systemctl restart rspamd`
Quién está bloqueado por fail2ban	`sudo fail2ban-client status dovecot` (o `postfix-sasl`)
Desbloquear una IP	`sudo fail2ban-client set dovecot unbanip LA_IP`

Si te atascas

Pega la línea `X-Spamd-Result` del correo, las últimas líneas de `/var/log/rspamd/rspamd.log` y la salida de `postconf smtpd_milters milter_protocol` .