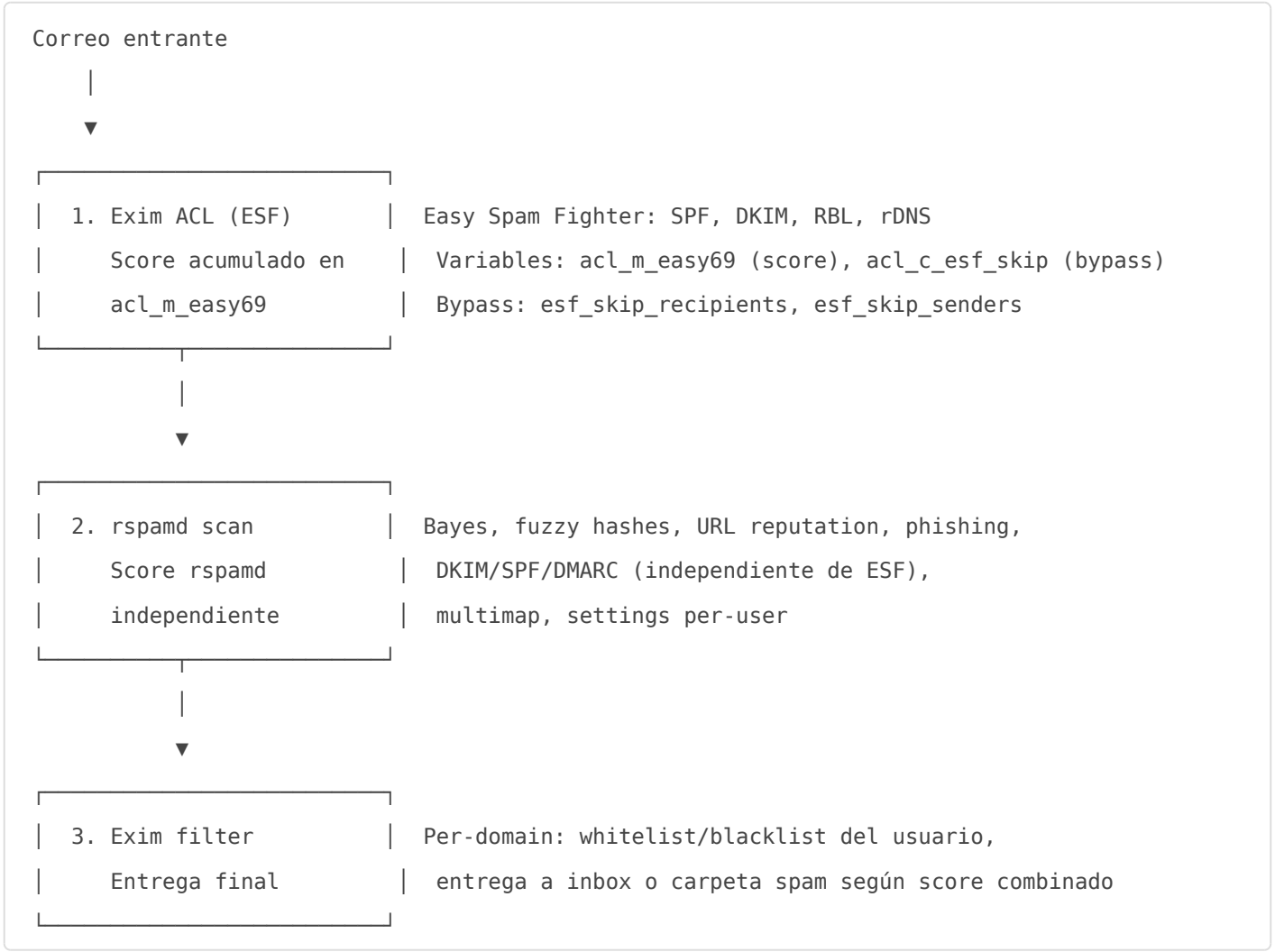
Arquitectura antispam en DirectAdmin: Exim ESF + rspamd

Las tres capas

DirectAdmin con rspamd activo procesa cada correo entrante en tres capas secuenciales:



Punto clave: ESF y rspamd son sistemas **independientes**. ESF evalúa en la ACL de Exim (antes de aceptar el correo), rspamd evalúa el contenido (después de aceptar). Cada uno genera su propio score. La decisión final la toma el filtro de dominio de Exim combinando ambos.

Capa 1: Easy Spam Fighter (ESF)

ESF es un conjunto de ACLs de Exim mantenido por DirectAdmin. Evalúa:

Check	Macro (default)	Qué hace
SPF pass	`EASY_SPF_PASS` (-30)	Bonificación por SPF válido
DKIM pass	`EASY_DKIM_PASS` (-20)	Bonificación por DKIM válido
rDNS confirmado	`EASY_FORWARD_CONFIRMED_RDNS` (-10)	Bonificación por PTR válido
SPF fail	`EASY_SPF_FAIL` (100)	Penalización por SPF inválido
DKIM fail	`EASY_DKIM_FAIL` (100)	Penalización por DKIM inválido
Sin rDNS	`EASY_NO_REVERSE_IP` (100)	Penalización por sin PTR
RBL hit	Variable	Penalización por blacklist
Acumulado default	**-60**	SPF+DKIM+rDNS válidos

El problema del -60

Un correo spam reenviado via Google Groups pasa SPF (google.com) + DKIM (google.com) + rDNS → obtiene **-60 puntos ESF** antes de que rspamd lo evalúe. Si rspamd devuelve un score bajo (no action), ESF no marca el correo y se entrega al INBOX.

Solución aplicada: reducir a -15 total (-5/-5/-5) via `variables.conf.custom`. Ver la página "Tuning de rspamd en DirectAdmin" para detalles.

Dónde se configuran los overrides ESF

```
/etc/exim.easy_spam_fighter/variables.conf         ← DA regenera (NO TOCAR)
/etc/exim.easy_spam_fighter/variables.conf.custom   ← Override seguro (== para redefinir)
```

Capa 2: rspamd

rspamd evalúa el contenido del correo de forma independiente:

- Bayes (aprendizaje estadístico)
- Fuzzy hashes (contenido conocido como spam)
- URL reputation (Spamhaus DBL, SURBL, URIBL)
- Phishing detection (OpenPhish)
- DKIM/SPF/DMARC (evaluación independiente de ESF)
- Multimap (whitelists, blacklists, penalizaciones custom)

- Settings per-user (thresholds, whitelists del panel)

Ficheros de configuración:

Ruta	Gestión	Seguro para editar
`/etc/rspamd/local.d/*.conf`	Manual	✅ Sí
`/etc/rspamd/local.d/maps/*.map`	Manual	✅ Sí
`/etc/rspamd/users.d/*.conf`	DirectAdmin	❌ No
`/etc/rspamd/directadmin-users.conf`	DirectAdmin	❌ No

Punto de unión: la condición de escaneo rspamd

El módulo rspamd de Exim (`/etc/exim/rspamd/check_message.conf`) tiene esta condición antes de escanear:

```
warn  condition = ${if eq{$acl_c_rspamd}{1}}
      condition = ${if !eq{$acl_c_esf_skip}{1}}      ← bypass ESF = bypass rspamd
      condition = ${if < {$message_size}{EASY_SPAMASSASSIN_MAX_SIZE}}
      condition = ${if !eq{$acl_m_spam_user}{nobody}}
      set acl_m_rspamd_on = 1
```

Cuatro condiciones deben cumplirse para que rspamd escanee:

1. `acl_c_rspamd = 1` — rspamd habilitado globalmente
2. `acl_c_esf_skip ≠ 1` — el dominio/remitente NO está en `esf_skip_*`
3. `message_size < MAX_SIZE` — correo dentro del límite (default 200K, recomendado 15M)
4. `acl_m_spam_user ≠ nobody` — el usuario tiene `~/.spamassassin/user_prefs`

Si **cualquiera** falla, rspamd NO escanea y el correo pasa sin evaluación de contenido.

Mecanismos de bypass

`esf_skip_recipients` y `esf_skip_senders`

Son **bypass TOTALES** — desactivan tanto el scoring ESF como el escaneo rspamd.

```
/etc/virtual/esf_skip_recipients   ← dominios destino (uno por línea)
/etc/virtual/esf_skip_senders      ← dominios remitente (uno por línea)
```

Cuando un dominio está en estos ficheros, `acl_c_esf_skip` se pone a 1 y rspamd no escanea.

Cuándo se usan: Como medida de protección para dominios con historial de falsos positivos graves que generaron fricción con el cliente. Es una decisión operativa consciente, no un mecanismo de "no rechazar".

Riesgo: Los correos que pasan por bypass no tienen NINGÚN escaneo — ni ESF ni rspamd ni phishing ni malware.

`acl_m_spam_user = nobody`

Si `~/.spamassassin/user_prefs` no existe para un usuario DA, la ACL no puede resolver el usuario y rspamd no escanea. Esto afecta silenciosamente a usuarios que nunca han tocado la configuración de SpamAssassin en el panel.

Diagnóstico:

```
# Contar correos sin escanear por user_prefs faltante
grep "acl_m_spam_user=nobody" /var/log/exim/mainlog | wc -l

# Listar usuarios sin user_prefs
for d in /home/*/; do
    user=$(basename "$d")
    if [ ! -f "$d/.spamassassin/user_prefs" ]; then
        echo "$user"
    fi
done
```

Solución: Crear `user_prefs` vacío con propietario correcto:

```
for d in /home/*/; do
    user=$(basename "$d")
    uid=$(id -u "$user" 2>/dev/null) || continue
    prefs_dir="$d/.spamassassin"
    prefs_file="$prefs_dir/user_prefs"
    if [ ! -f "$prefs_file" ]; then
        mkdir -p "$prefs_dir"
        touch "$prefs_file"
```

```
        chown -R "$user:$user" "$prefs_dir"
    fi
done
```

`EASY_SPAMASSASSIN_MAX_SIZE`

Default: 200K. Correos con adjuntos (>200K) no se escanean. Recomendado: 15M.

```
# En variables.conf.custom
EASY_SPAMASSASSIN_MAX_SIZE == 15M
```

Alternativas a bypass total

Para casos donde se necesita proteger contra falsos positivos SIN perder el escaneo rspamd:

Mecanismo	Qué hace	rspamd escanea	Riesgo
`esf_skip_*`	Bypass total	No	Sin protección alguna
`whitelist_from.map` (score -100)	Whitelist rspamd	Sí	Bajo (detecta phishing/malware)
Whitelist dinámica (via email)	Whitelist rspamd	Sí	Bajo
Per-user threshold alto	Threshold permisivo	Sí	Medio (score alto pasa)

Recomendación: Para nuevos casos de "no rechazar", usar `whitelist_from.map` con score -100. rspamd escanea (phishing, malware, URLs), pero el score se neutraliza.

Diagrama de decisión: ¿por qué no se escaneó?

```
¿rspamd escaneó este correo?
    │
    ├── NO → ¿acl_c_esf_skip = 1?
    │         ├── SÍ → Dominio en esf_skip_recipients o esf_skip_senders
    │         └── NO → ¿message_size > MAX_SIZE?
    │                   ├── SÍ → Correo demasiado grande (subir MAX_SIZE)
    │                   └── NO → ¿acl_m_spam_user = nobody?
```

```
    │                          ├── SÍ → user_prefs no existe (crear)
    │                          └── NO → ¿acl_c_rspamd = 0?
    │                                    ├── SÍ → rspamd desactivado globalmente
    │                                    └── NO → Investigar ACLs
    │
    └── SÍ → ¿Por qué pasó?
              ├── Score bajo → Revisar Bayes, multimap, thresholds
              ├── Whitelist activa → Revisar whitelist_from.map + dynamic
              └── ESF score muy negativo → Reducir scores ESF (variables.conf.custom)
```

Diagnóstico rápido

```
# 1. ¿rspamd escaneó? Buscar cabeceras en el correo
grep "X-Spamd-Result" /path/to/email

# 2. ¿Cuántos correos no se escanearon esta semana?
# Por esf_skip:
grep "esf_skip" /var/log/exim/mainlog | wc -l

# Por user nobody:
grep "spam_user=nobody" /var/log/exim/mainlog | wc -l

# Por tamaño:
grep "too large for spam" /var/log/exim/mainlog | wc -l

# 3. ¿Qué dominios tienen bypass activo?
cat /etc/virtual/esf_skip_recipients
cat /etc/virtual/esf_skip_senders

# 4. Estado de Bayes (usar controller socket en DA)
rspamc --connect /var/run/rspamd/rspamd_controller.sock stat

# 5. Volumen spam vs ham
rspamc --connect /var/run/rspamd/rspamd_controller.sock stat | grep -E "Messages
scanned|Spam|Ham"
```

Resumen de configuración de referencia

Tras aplicar el tuning completo documentado en esta wiki:

Componente	Configuración	Fichero
ESF scores	-5/-5/-5 (total -15)	`variables.conf.custom`
ESF max_size	15M	`variables.conf.custom`
ESF high_score_drop	9999 (nunca)	`variables.conf.custom`
rspamd reject	null (nunca)	`actions.conf`
rspamd add_header	5 (marcar)	`actions.conf`
Bayes backend	Redis (pool global)	`classifier-bayes.conf`
Bayes autolearn	spam ≥8.0, ham ≤-1.0	`classifier-bayes.conf`
Phishing	OpenPhish activo	`phishing.conf`
URL suspect	word_dot desactivado	`url_suspect.conf`
Whitelist estática	score -100, filter=email:domain	`multimap.conf`
Whitelist dinámica	Via email, score -100	`multimap.conf`
DNSBL resolvers	64.6.64.6 / 199.85.126.10 / 156.154.70.2	netplan

Revision #1
Created 2026-03-24 17:34:56 UTC by Abkrim
Updated 2026-03-24 17:34:56 UTC by Abkrim