Microsoft S775: sacar el correo por un smarthost en cPanel (todo el servidor o solo hacia Microsoft)

El problema

Microsoft limita a veces la entrega desde una IP por su reputación. Los mensajes hacia Hotmail, Outlook, Live, MSN **y hacia cualquier empresa con correo en Microsoft 365** se quedan en cola con este error:

```
451 4.7.650 The mail server [192.0.2.10] has been temporarily rate limited due to IP
reputation.
For e-mail delivery information, see https://aka.ms/postmaster (S775)
```

El rechazo llega ya en el `MAIL FROM`, antes de enviar el mensaje. Es temporal (`451`), así que Exim reintenta y el correo se acumula en la cola sin rebotar durante horas.

En el caso que dio origen a esta guía no había nada anómalo en el servidor: ninguna cuenta comprometida, un volumen normal y la IP fuera de las listas negras habituales. La reputación había caído por el rango de IP, no por un envío concreto. Mientras se tramita la revisión con Microsoft, el correo tiene que salir por otra IP: un smarthost en un rango limpio.

Esta guía recoge dos formas de hacerlo en cPanel:

- **Variante A — todo el correo saliente por el smarthost.** Es la nativa de cPanel, tarda un minuto y es la que estuvo en producción en el caso real, durante tres días y sin incidencias.
- **Variante B — solo el correo cuyo destino usa Microsoft.** El resto sale directo por la IP del servidor. La lógica de enrutado está validada en laboratorio; su despliegue en cPanel no se ha probado todavía en producción (lo explico en su apartado).

Si buscas rutas por dominio de destino con varios smarthosts, mira Rutas Específicas o smarthost complejo para Exim y cPanel.

Diagnóstico previo (común)

Confirma que el problema es la IP y no un envío del servidor antes de tocar nada.

```
# ¿Desde cuándo aparece el S775 y a cuántos mensajes afecta?
grep 'S775' /var/log/exim_mainlog | head -1
grep 'S775' /var/log/exim_mainlog | awk '{print $3}' | sort -u | wc -l

# Prueba directa desde la IP del servidor, sin enviar ningún mensaje
python3 - <<'EOF'
import smtplib, socket
ip = socket.gethostbyname("hotmail-com.olc.protection.outlook.com")
s = smtplib.SMTP(timeout=30, source_address=("192.0.2.10", 0))
print(s.connect(ip, 25)); s.ehlo("servidor.example.com")
print(s.mail("prueba@example.com"))
s.quit()
EOF
```

Cambia `192.0.2.10` por la IP de salida del servidor. Si el `MAIL FROM` responde `451 4.7.650 … (S775)`, el bloqueo es de la IP.

En paralelo, solicita la revisión de la IP a Microsoft desde su formulario de soporte para remitentes. La primera respuesta suele ser automática («Not qualified for mitigation»): hay que insistir pidiendo revisión manual. En el caso real, el técnico pidió una captura del error SMTP con fecha y hora de las últimas 36 horas, y la prueba anterior sirve exactamente para eso.

SPF: un include fijo para todo el pool de smarthosts (común)

El SPF de **todos** los dominios que envían desde el servidor debe autorizar a los smarthosts. Si no lo hace, los receptores marcarán los mensajes como fallo de SPF en cuanto se desvíe el correo.

La forma que recomiendo es no apuntar a un smarthost concreto, sino a un registro propio que liste **todo el pool**, y que cada dominio lo incluya de forma permanente:

```
; registro central, mantenido por el administrador de los smarthosts
_smarts.example.net.  TXT  "v=spf1 ip4:198.51.100.11 ip4:198.51.100.12 ip4:198.51.100.13 ~all"

; SPF de cada dominio cliente
example.com.          TXT  "v=spf1 a mx include:_smarts.example.net ~all"
```

- **Los dominios quedan preparados de antemano.** Si mañana hay que desviar el correo, el SPF ya está listo y no hay que esperar a que caduque ningún TTL.
- **El pool puede crecer sin tocar el DNS de los clientes.** Añadir o retirar smarthosts es editar un solo registro. En temporadas de muchos bloqueos he llegado a necesitar ocho.
- **Vigila el límite de 10 consultas DNS del SPF:** el `include` cuenta una, y el registro central debe usar `ip4:` y no más `include`.
- Coloca el `include` antes del `all`.

Para añadirlo a todos los dominios de un servidor: Cómo añadir una entrada SPF a todos los dominios de un servidor cPanel.

El `include` se queda puesto también después del incidente: es parte del diseño, no un parche temporal.

Varios smarthosts en la ruta

En las dos variantes, la ruta admite varios smarthosts separados por `:`. Exim prueba el siguiente si uno no responde, y con `hosts_randomize = true` reparte la carga entre ellos:

```
route_list = * smart1.example.net:smart2.example.net:smart3.example.net
```

En la variante A eso va en el mismo campo de cPanel (`smarthost_routelist=* smart1.example.net:smart2.example.net`). En la variante B, añade `hosts_randomize = true` a cada router.

Variante A — todo el correo saliente por el smarthost

Es la opción nativa de cPanel: **WHM → Service Configuration → Exim Configuration Manager → Basic Editor → Routing → Smarthost support**. Por línea de comandos es la clave `smarthost_routelist` de `/etc/exim.conf.localopts`.

```
TS=$(date +%Y%m%d%H%M%S)
cp -a /etc/exim.conf.localopts /etc/exim.conf.localopts.bak-$TS
cp -a /etc/exim.conf /etc/exim.conf.bak-$TS

sed -i 's/^smarthost_routelist=.*/smarthost_routelist=* smart.example.net/'
/etc/exim.conf.localopts
/scripts/buildeximconf && /scripts/restartsrv_exim

# Verificación
grep -c 'smart.example.net' /etc/exim.conf      # 5 routers apuntando al smarthost
exim -bt usuario@hotmail.com                    # host smart.example.net
exim -bt usuario@gmail.com                      # también por el smarthost
```

Después, empuja la cola retenida (`exim -qff`) y comprueba en el log que las entregas a Hotmail se aceptan con `250`.

> **Importante: la lista de rutas de cPanel no sirve para filtrar solo Microsoft.** Con smarthost, cPanel convierte los cuatro routers de salida (`dkim_lookuphost`, `lookuphost` y sus variantes de autorrespuesta) en `manualroute` con **la misma** lista. Si pones `smarthost_routelist` solo con dominios de Microsoft, cualquier otro destino se queda sin router y rebota con `Unrouteable address`. Lo he reproducido en laboratorio: Hotmail salía por el smarthost, y Gmail y el resto quedaban sin ruta. Para filtrar por destino, usa la variante B.

Desactivar la variante A

Cuando Microsoft relaje la restricción, repite la prueba directa del diagnóstico. Si responde `250 2.1.0 Sender OK`, vuelve a la entrega directa:

```
TS=$(date +%Y%m%d%H%M%S)
cp -a /etc/exim.conf.localopts /etc/exim.conf.localopts.bak-$TS
cp -a /etc/exim.conf /etc/exim.conf.bak-$TS
sed -i 's/^smarthost_routelist=.*/smarthost_routelist=/' /etc/exim.conf.localopts
/scripts/buildeximconf && /scripts/restartsrv_exim

grep -c 'smart.example.net' /etc/exim.conf      # 0
exim -bt usuario@hotmail.com                    # MX de Microsoft directamente
```

Al regenerar puede aparecer `SMTP Mail protection has been disabled`. Si la restricción de salida la aplica CSF (`SMTP_BLOCK = "1"`), es lo esperado: cPanel la deja en manos del firewall. Revisa en el log las primeras entregas reales hacia Microsoft desde la IP propia. Si vuelve el `451`, restaura el backup.

Variante B — solo el correo cuyo destino usa Microsoft

Un router propio, colocado antes que los de cPanel, que **mira el MX del dominio de destino**. Si el MX es de la protección de Exchange Online (`*.protection.outlook.com`), manda el mensaje al smarthost. Si no, el router no actúa y el mensaje sigue por los routers normales de cPanel, en entrega directa.

Filtrar por MX y no por dominio es la clave. El `S775` lo aplica Exchange Online Protection a todos sus clientes, y una lista con `hotmail.com`, `outlook.com`, `live.com` y `msn.com` deja fuera a cualquier empresa con Microsoft 365 en su propio dominio, cuyo MX es `<dominio>.mail.protection.outlook.com`.

El router

En **WHM → Exim Configuration Manager → Advanced Editor**, sección `ROUTERSTART`:

```
microsoft_smarthost_dkim:
  driver = manualroute
  domains = ! +local_domains
  condition = ${if match{${lookup dnsdb{>:
mx=$domain}{$value}{}}}{\N(?i)\.protection\.outlook\.com\.?(:|$)\N}}
  condition = "${perl{sender_domain_can_dkim_sign}}"
  route_list = * smart.example.net
  transport = dkim_remote_smtp

microsoft_smarthost:
  driver = manualroute
  domains = ! +local_domains
  condition = ${if match{${lookup dnsdb{>:
mx=$domain}{$value}{}}}{\N(?i)\.protection\.outlook\.com\.?(:|$)\N}}
  route_list = * smart.example.net
  transport = remote_smtp
```

Son dos routers por la misma razón que cPanel duplica los suyos: el primero entrega con el transporte que firma DKIM si el dominio remitente tiene clave, y el segundo cubre el resto.

Si la consulta del MX falla (error temporal de DNS), la condición no casa y el mensaje sale directo. El router nunca deja un mensaje sin ruta.

Guarda el editor. WHM valida y regenera `/etc/exim.conf`; si hay un error de sintaxis, conserva la configuración anterior.

Qué está validado y qué no

He validado la lógica de enrutado con Exim 4.98 en un laboratorio aislado, con DNS real. Resultado con `exim -bt`:

Destino	MX	Router	Salida
`hotmail.com`, `outlook.es`, `live.com`, `msn.com`	`*.olc.protection.outlook.com`	`microsoft_smarthost`	smarthost
`microsoft.com` (Microsoft 365 corporativo)	`*.mail.protection.outlook.com`	`microsoft_smarthost`	smarthost
dominio con MX de Proofpoint	`*.pphosted.com`	`lookuphost`	directa
`gmail.com`	`gmail-smtp-in.l.google.com`	`lookuphost`	directa

No se ha probado todavía en un cPanel en producción: el comportamiento dentro de `ROUTERSTART` junto al resto de routers de cPanel y la firma DKIM a través de `dkim_remote_smtp`. El Exim de cPanel no permite cargar una configuración alternativa con `-C`, así que la única prueba posible es en el propio servidor. Hazlo en una ventana tranquila, con backup y con esta verificación:

```
exim -bt usuario@hotmail.com           # router = microsoft_smarthost(_dkim), host
smart.example.net
exim -bt usuario@empresa-con-m365.com  # igual, si su MX es *.mail.protection.outlook.com
exim -bt usuario@gmail.com             # router = dkim_lookuphost o lookuphost, MX de Google
```

Después, envía un mensaje real a un buzón de Hotmail tuyo y revisa en sus cabeceras que `DKIM-Signature` está presente y que `Authentication-Results` dice `dkim=pass` y `spf=pass`.

Desactivar la variante B

Borra los dos routers del Advanced Editor y guarda. Comprueba con `exim -bt usuario@hotmail.com` que vuelve a resolver a los MX de Microsoft.

Cuál elegir

	Variante A	Variante B
Qué desvía	Todo el correo saliente	Solo destinos con MX de Microsoft
Configuración	Nativa de cPanel, un campo	Dos routers en el Advanced Editor
Riesgo	Todo depende del smarthost	Si el router falla, el resto no se entera
Estado	En producción, sin incidencias	Lógica validada en laboratorio
Cuándo	Emergencia: el correo tiene que salir ya	Bloqueos repetidos o largos, o un smarthost con capacidad limitada

En una emergencia, la variante A es la más rápida y la que menos puede fallar. Si el bloqueo se alarga, o si el smarthost no debería cargar con todo el tráfico, la variante B reduce el desvío a lo imprescindible.

Aviso

Esta documentación y su contenido no implican que funcione en tu caso o en determinados casos. También implica que tienes conocimientos sobre lo que trata y que, en cualquier caso, tienes copias de seguridad. El contenido se entrega tal y como está, sin que ello implique ninguna obligación ni responsabilidad por parte de Castris.

Si necesitas soporte profesional, puedes contratarlo con Castris: soporte profesional.

Revision #1
Created 2026-11-23 18:53:23 UTC by Abkrim
Updated 2026-11-23 18:53:24 UTC by Abkrim