Postfix Smart Relay en casos de bloqueo puerto 25 - Configuración Completa

Escenario

Servidor sin panel de control que necesita enviar correos electrónicos (alertas, notificaciones) pero tiene el puerto 25 bloqueado por el ISP (Hetzner). Solución mediante smart relay a otro servidor Postfix actuando como gateway de salida.

Configuración Postfix Smart Relay - Puerto 25 Bloqueado

Escenario

Servidor sin panel de control que necesita enviar correos electrónicos (alertas, notificaciones) pero tiene el puerto 25 bloqueado por el ISP (Hetzner). Solución mediante smart relay a otro servidor Postfix actuando como gateway de salida.

Arquitectura

```
[Servidor Origen] --puerto 587--> [Smart Relay] --puerto 25--> [Internet]
   (puerto 25 capado)              (múltiples ubicaciones)
```

Configuración del Servidor Origen (Cliente)

1. Instalación básica

```
apt-get install postfix mailutils
```

2. Configuración main.cf

```
# /etc/postfix/main.cf

# ⚠ CRÍTICO: Verificar sintaxis exacta - errores tipográficos causan bucles
myhostname = alerts.tudominio.com
mydomain = tudominio.com
myorigin = alerts.tudominio.com  # Debe coincidir exactamente con DKIM

# Smart relay
relayhost = [ip-smart-relay]:587

# Configuración local mínima
inet_interfaces = loopback-only
mydestination = localhost, localhost.localdomain
local_recipient_maps =
local_transport = error:local mail delivery is disabled

# ⚠ IMPORTANTE: Incluir TODAS las IPs que pueden enviar bounces
mynetworks = 127.0.0.0/8 [::1]/128 [IP-smart-relay]

# TLS para conexión al smart relay
smtp_use_tls = yes
smtp_tls_security_level = encrypt

# ⚠ NUEVO: Transport maps para evitar bucles de bounces
transport_maps = hash:/etc/postfix/transport
```

3. Transport maps (CRÍTICO para evitar bucles)

```
# /etc/postfix/transport
# Mantener correos hacia el propio dominio locales para evitar bucles
alerts.tudominio.com    local:

# Compilar
postmap /etc/postfix/transport
```

4. Aliases básicos

```
# /etc/aliases
root: sysadmin@tudominio.com
postmaster: sysadmin@tudominio.com
# Usuario para descartar bounces automáticos
devnull: /dev/null

# Aplicar cambios
newaliases
postfix reload
```

Configuración del Smart Relay

1. Configuración main.cf del smart relay

```
# /etc/postfix/main.cf

# Configuración básica
myhostname = smart-relay.tudominio.com
mydomain = tudominio.com

# ⚠ CRÍTICO: Permitir relay desde IPs específicas
mynetworks = 127.0.0.0/8 [::1]/128 [IP-cliente-1] [IP-cliente-2]
```

```
# Configuración de relay
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated
defer_unauth_destination

# TLS
smtpd_use_tls = yes
smtpd_tls_cert_file = /etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file = /etc/ssl/private/ssl-cert-snakeoil.key
```

2. Puerto alternativo en master.cf

```
# /etc/postfix/master.cf

# Puerto estándar
smtp      inet  n       -       y       -       -       smtpd

# Puerto alternativo para clientes con puerto 25 capado
587       inet  n       -       y       -       -       smtpd
  -o smtpd_client_restrictions=permit_mynetworks,reject
  -o smtpd_tls_security_level=encrypt
```

3. Gestión de bounces (Prevención de bucles)

```
# /etc/aliases en smart relay
devnull: /dev/null
bounces: /dev/null

# Aplicar
newaliases
```

Configuración DNS y Autenticación

1. SPF Record

```
; Para el dominio principal
tudominio.com. IN TXT "v=spf1 ip4:ip-smart-relay-1 ip4:ip-smart-relay-2 -all"

; Para subdominios específicos (IMPORTANTE)
alerts.tudominio.com. IN TXT "v=spf1 ip4:ip-smart-relay-1 ip4:ip-smart-relay-2 -all"
```

2. DKIM Configuration

```
# Instalar herramientas DKIM
apt-get install opendkim opendkim-tools

# Generar claves
opendkim-genkey -t -s mail -d alerts.tudominio.com

# ⚠ IMPORTANTE: El selector debe coincidir con el dominio usado en myorigin
```

3. DMARC Policy

```
_dmarc.tudominio.com. IN TXT "v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@tudominio.com"
```

Resolución de Problemas Críticos

1. Bucles de correo ("too many hops")

Síntoma: Error 5.4.0 "too many hops" **Causa**: Correos hacia el propio dominio van al smart relay y vuelven

Solución:

```
# /etc/postfix/transport en servidor origen
alerts.tudominio.com    local:
```

```
# Recompilar
postmap /etc/postfix/transport
systemctl reload postfix
```

2. "Relay access denied"

Síntoma: 454 4.7.1 Relay access denied **Causa**: IP del cliente no está en mynetworks del smart relay

Diagnóstico:

```
# En smart relay, verificar qué IP se conecta
grep "connect from" /var/log/mail.log | grep [IP-problema]

# Verificar configuración actual
postconf mynetworks
```

Solución: Añadir IP faltante a mynetworks

3. Alias no funciona

Síntoma: Los alias no se aplican correctamente **Causa común**: Errores tipográficos en myorigin

Diagnóstico:

```
# Verificar que el alias funciona
postalias -q root /etc/aliases

# ⚠ VERIFICAR EXACTITUD de myorigin
postconf myorigin

# Común: "alertas" vs "alerts", ".co" vs ".com"
```

4. DKIM/DMARC failures

Síntoma: Correos marcados como spam **Causa**: Desalineación entre From domain y SPF/DKIM

Solución: Asegurar que myorigin coincide exactamente con dominio DKIM

Testing y Verificación

1. Test de funcionamiento básico

```
# Test desde línea de comandos
echo "Test desde $(hostname)" | mail -s "Test Relay" destino@gmail.com

# Verificar logs inmediatamente
tail -f /var/log/mail.log
```

2. Test de alias

```
# Envío a root debe ir al alias configurado
echo "Test alias" | mail -s "Test root alias" root

# Verificar en logs que va al destino correcto
```

3. Verificación DNS

```
# SPF
dig TXT alerts.tudominio.com

# DKIM
dig TXT mail._domainkey.alerts.tudominio.com

# DMARC
dig TXT _dmarc.tudominio.com
```

Errores Comunes y Soluciones

Error: myorigin con tipografías

```
# MAL
myorigin = alertas.avanzait.co  # ← error tipográfico

# BIEN
myorigin = alerts.avanzait.com
```

Error: mynetworks incompleto

```
# MAL - falta IP del smart relay
mynetworks = 127.0.0.0/8

# BIEN - incluye smart relay para bounces
mynetworks = 127.0.0.0/8 [IP-smart-relay]
```

Error: Sin transport maps

Sin transport maps, los correos al propio dominio crean bucles.

Configuración correcta

```
# main.cf
transport_maps = hash:/etc/postfix/transport

# /etc/postfix/transport
alerts.tudominio.com    local:
```

Configuración para Aplicaciones Específicas

Zabbix

```
# Media Type configuración
SMTP server: localhost
Port: 25
Email: root@alerts.tudominio.com
Authentication: None
Security: None
```

CSF (ConfigServer Firewall)

Los correos de sistema funcionarán automáticamente una vez configurados los alias correctamente. Eso incluye pruebas de concepto, avisos de CSF, etc.

Aplicaciones web (PHP/Python)

```
// PHP
ini_set('SMTP', 'localhost');
ini_set('smtp_port', 25);
```

Monitoreo y Mantenimiento

1. Script de monitoreo de colas

```
#!/bin/bash
# /usr/local/bin/check-mail-queue.sh
QUEUE_SIZE=$(mailq | tail -1 | awk '{print $5}' | tr -d ')')
if [ "$QUEUE_SIZE" -gt 50 ]; then
    echo "ALERT: Mail queue size: $QUEUE_SIZE" | \
    mail -s "Mail Queue Alert" admin@tudominio.com
fi
```

2. Verificación periódica de configuración

```
#!/bin/bash
# Verificar configuraciones críticas
```

```
echo "=== Verificación Postfix ==="
echo "myorigin: $(postconf myorigin)"
echo "relayhost: $(postconf relayhost)"
echo "mynetworks: $(postconf mynetworks)"
echo "transport_maps: $(postconf transport_maps)"
```

3. Backup de configuración

```
# Script de backup
tar -czf /backup/postfix-config-$(date +%Y%m%d).tar.gz \
    /etc/postfix/ \
    /etc/aliases \
    /etc/opendkim/ 2>/dev/null
```

Lista de Verificación Pre-Producción

- ☐ `myorigin` sin errores tipográficos
- ☐ `mynetworks` incluye todas las IPs necesarias
- ☐ `transport_maps` configurado para evitar bucles
- ☐ Aliases funcionando (`postalias -q root /etc/aliases`)
- ☐ SPF record publicado
- ☐ DKIM keys generados y DNS configurado
- ☐ DMARC policy establecida
- ☐ Test de envío exitoso
- ☐ Logs sin errores de relay
- ☐ Smart relay acepta conexiones del cliente

Troubleshooting Rápido

Bucle detectado

1. Verificar `myorigin` (sin typos)
2. Configurar `transport_maps`
3. Verificar `mynetworks` en ambos servidores

Alias no funciona

1. Verificar `/etc/aliases`
2. Ejecutar `newaliases`
3. Verificar con `postalias -q`

Relay denied

1. Verificar IP real de conexión en logs
2. Añadir IP a `mynetworks` del smart relay
3. Reload postfix

Aviso Legal

Esta documentación se proporciona "tal como está" sin garantías. Se recomienda realizar pruebas exhaustivas y mantener copias de seguridad.

Para soporte profesional: Castris Soporte

Revision #2
Created 2025-09-18 06:44:05 UTC by Abkrim
Updated 2025-09-18 10:05:50 UTC by Abkrim