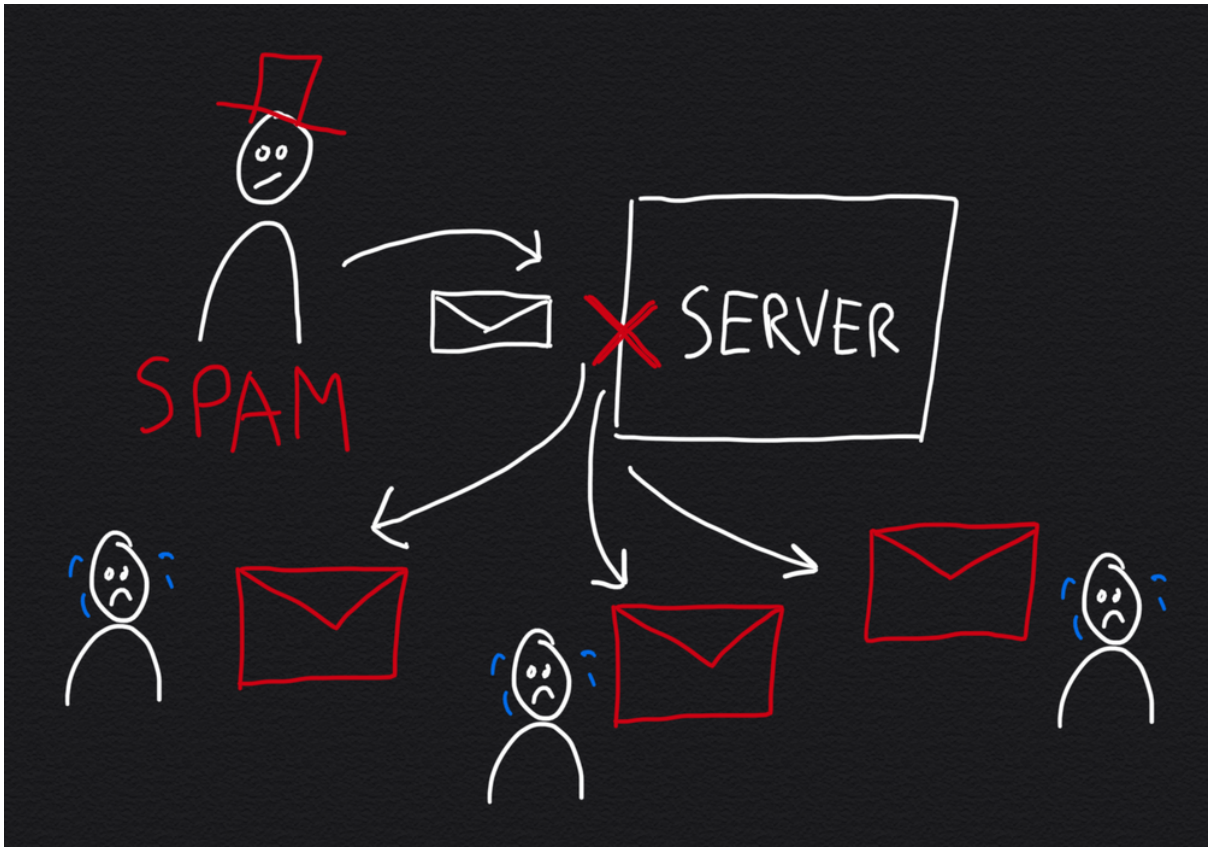
Combatir el spam de retrodispersión a nivel de servidor

Configurar Postfix para bloquear el spam antes de que entre al servidor

Willem L. Middelkoop
Sep. 10, 2019



Este mes tuve que lidiar con spam de retrodispersión, afectando a uno de los servidores de correo que administro. Como ingeniero de servidores, me aseguro de que los servidores no envíen spam y de que el correo electrónico entrante se filtre. A pesar de todos los esfuerzos, este servidor seguía estando en la lista negra por enviar spam a iCloud, Office 365 y Google Gmail para empresas (G Suite). Sigue leyendo para descubrir qué causó esto y cómo solucionarlo.

El problema

El servidor es un servidor de correo Postfix en Debian GNU/Linux que ejecuta todas las actualizaciones y parches de seguridad más recientes. El servidor es utilizado por clientes

legítimos que solo pueden usarlo con la autenticación adecuada.

Evitar ser un open relay

La autenticación de usuario individual en un servidor de correo es una medida importante contra el abuso del servidor de correo. Si se envía spam, puede ver qué usuario está causando el problema mirando los registros del servidor de correo. En términos técnicos, esto significa que evita que el servidor se convierta en 'un open relay'. Postfix ofrece muchas configuraciones para limitar el reenvío SMTP mediante el control de acceso.

Limitación de tasa de envío para cuentas de correo (hackeadas)

El abuso del servidor por parte de usuarios individuales ocurre cuando su computadora contrae un virus o cuando su contraseña es interceptada. Eso puede suceder cuando accede a su correo a través de una red WiFi insegura sin cifrado (TLS/SSL). Para situaciones como esta, es una buena idea limitar la cantidad de correos electrónicos que los usuarios individuales pueden enviar. Puede usar parámetros_de_configuración_de_Postfix individuales (como *smtpd_client_message_rate_limit, smtpd_client_connection_rate_limit* y *smtpd_client_recipient_rate_limit*) o usar un firewall de Postfix como Postwfd.

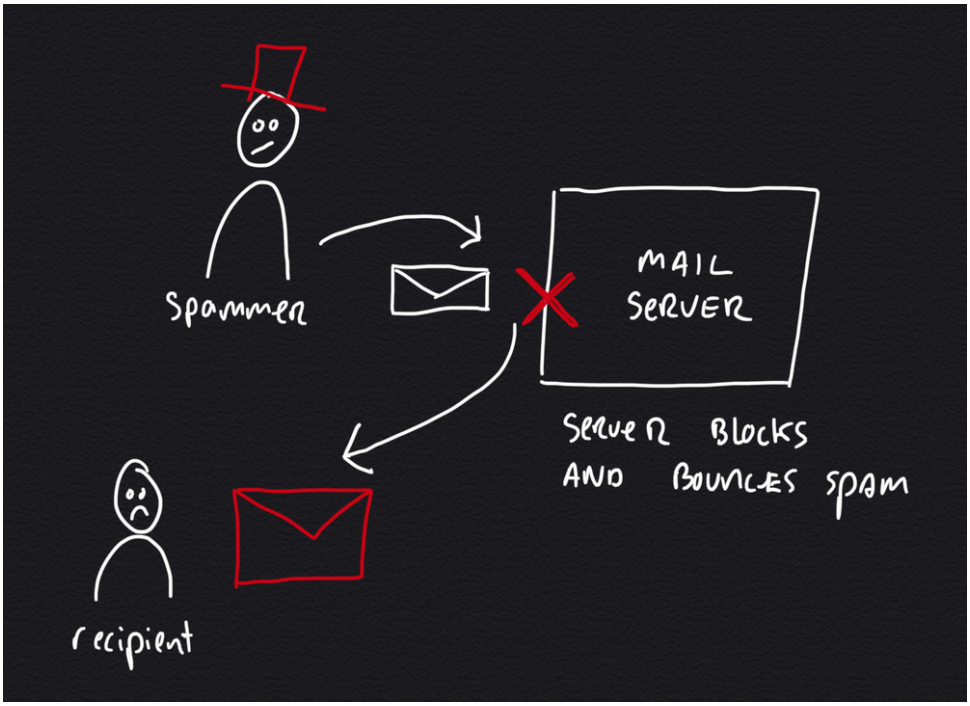
El servidor aparece en la lista negra de 'backscatterer.org'

A pesar de todas las medidas contra el abuso de spam, el servidor aún figuraba en `http://backscatter.org` por enviar spam. Si un servidor aparece en una lista negra, otros servidores ya no confiarán en él y considerarán que todos los mensajes son sospechosos. Esto puede causar que sus mensajes (legítimos) sean vistos por otros servidores como spam (falsos positivos). Para entender por qué sucedió esto, primero debe comprender qué es el spam de backscatter.

¿Qué es el spam de Backscatter?

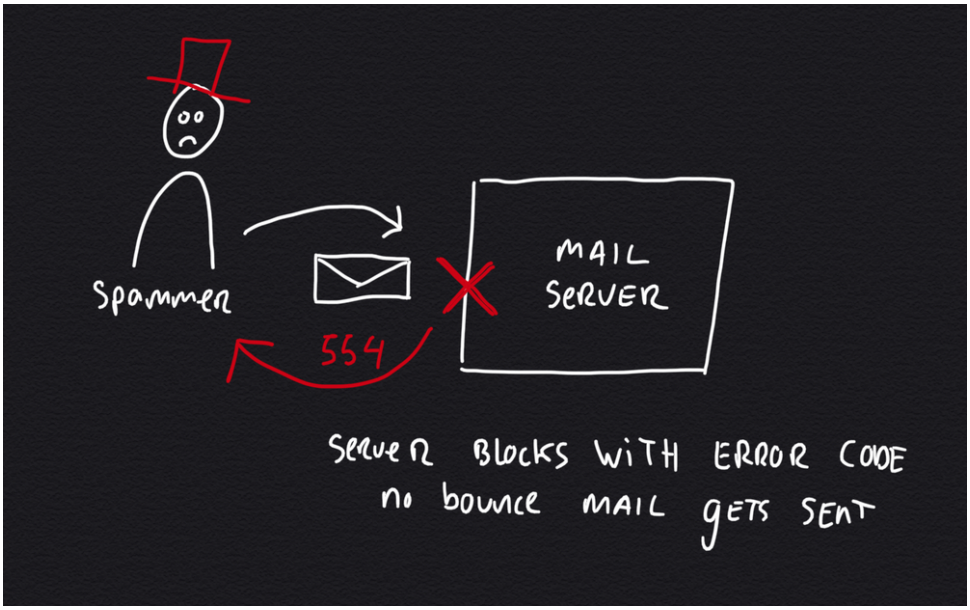
El spam de backscatter son mensajes de rebote automatizados incorrectamente enviados por el servidor de correo, generalmente como un efecto secundario del spam entrante.

El backscatter ocurre cuando los spammers falsifican la dirección del remitente. Envían un mensaje de correo que esperan que rebote utilizando la dirección de otra persona como remitente. Cuando el mensaje de correo rebota, el servidor de correo devuelve el mensaje al remitente falsificado... lo que hace que el servidor entregue spam a la dirección del remitente.



Escenario simple de backscatter, el servidor de correo devuelve el mensaje a una dirección de remitente falsificada

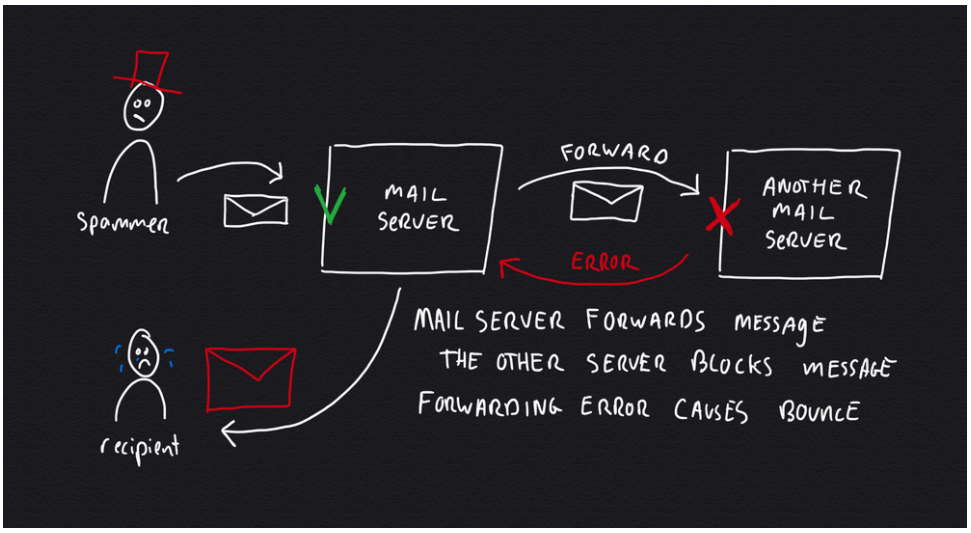
El escenario simple de backscatter es donde un mensaje rebota al remitente incorrecto. Es un escenario que es simple de resolver configurando el servidor para que no envíe mensajes de rebote, sino que responda con un código de error SMTP.



Evite los mensajes de rebote de backscatter respondiendo con códigos de error SMTP

Desafortunadamente, hay otro escenario (más difícil) que hace que su servidor de correo envíe spam de backscatter. Esto sucede cuando alguien en su servidor configura su cuenta de correo para reenviar el correo electrónico a otra dirección. El segundo servidor podría tener un filtro de spam más estricto que hace que los mensajes se bloqueen

al reenviar. Su servidor de correo informará al remitente original que el reenvío falló, causando spam de backscatter.

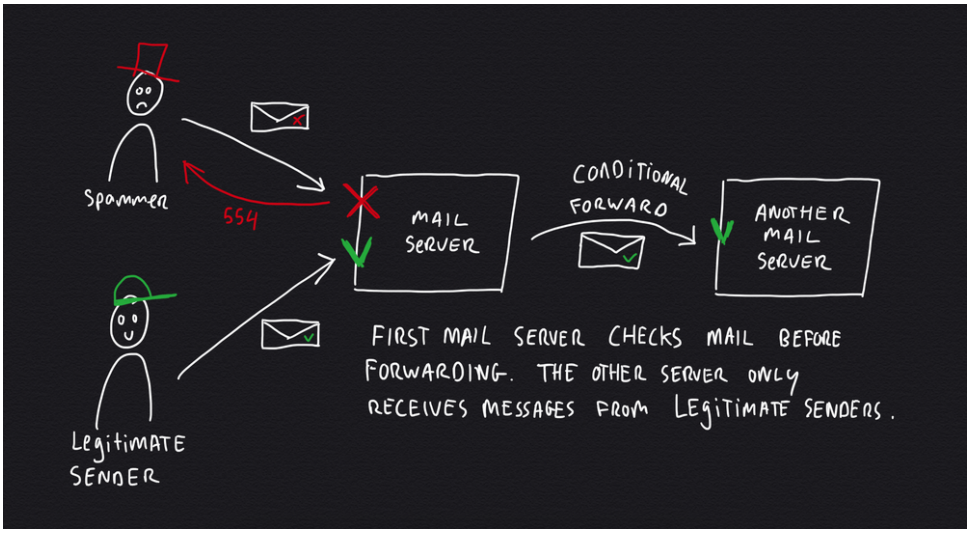


Causando spam de backscatter cuando el primer servidor de correo reenvía el correo electrónico a otro servidor que bloquea el mensaje

El escenario de reenvío es mucho más difícil de resolver, ya que posiblemente no controle el otro servidor de correo o la configuración de su filtro de spam. Lo que es peor es que a menudo hay un retraso entre la aceptación del mensaje y su reenvío, lo que hace que sea imposible esperar una respuesta del otro servidor de correo.

Prevenir el spam de backscatter

La única forma en que puede prevenir completamente el spam de backscatter es ser muy estricto en el primer servidor de correo, en la etapa inicial de conexión SMTP. Esto resuelve el desafiante 'escenario de reenvío' al ser muy selectivo con los mensajes que se reenvían.



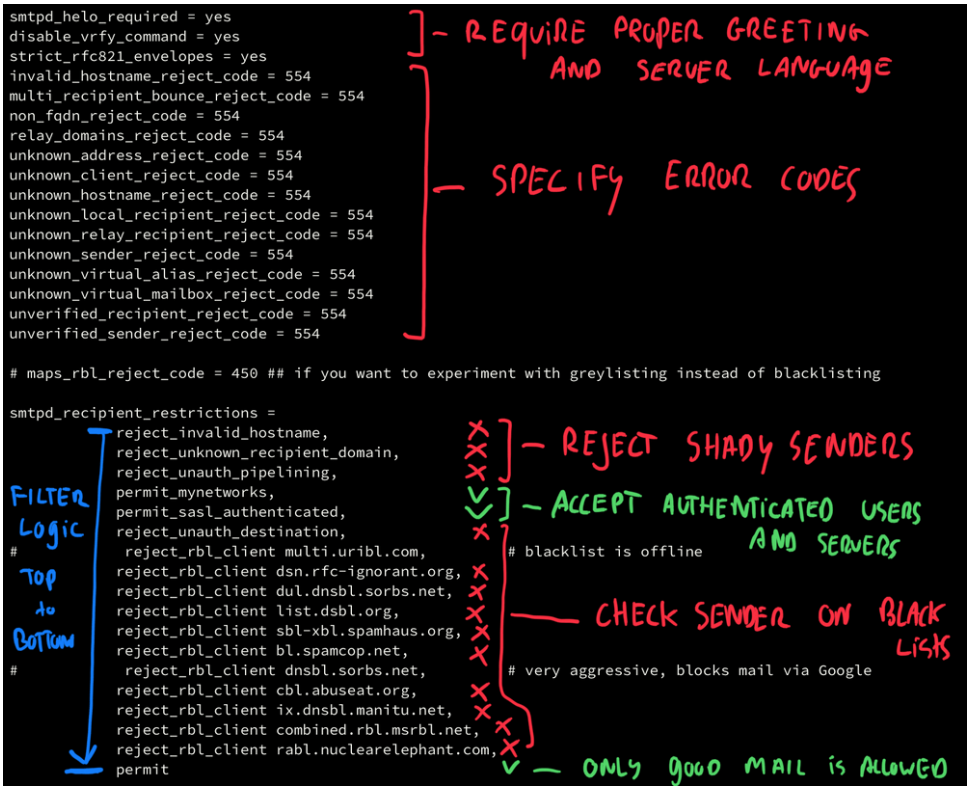
Evite el spam de backscatter comprobando todos los mensajes antes de reenviarlos a otro servidor

Cómo bloquear el spam antes de que ingrese al servidor

La mejor manera de prevenir el spam de backscatter es bloquearlo antes de que ingrese a la (cadena de) servidor(es).

Tradicionalmente, los servidores utilizan filtros de spam avanzados como SpamAssasin para analizar los mensajes uno por uno. Esto causa una carga adicional en el servidor de correo.

Es mucho más fácil mirar al remitente (por ejemplo, si usa un sombrero rojo) para el filtrado inicial. ¿Está el remitente en una lista negra? ¿Utiliza una aplicación de correo 'normal' o los mensajes los envía un virus o malware? Puede determinar muchas cosas observando el 'idioma' que habla el remitente.



Implementando restricciones SMTP estrictas en Postfix - captura de pantalla anotada de main.cf

En Postfix, puede especificar restricciones SMTP en el archivo de configuración *main.cf*. Hay comprobaciones que se pueden utilizar para bloquear mensajes. Es una buena idea trabajar de 'fácil a difícil' en la lógica del filtro, comenzando con cosas que se pueden verificar sin consultar servidores externos. Esto reduce el tráfico de red y la carga. Solo si un mensaje pasa todas las comprobaciones, se permite su entrega (o reenvío).

Tras la entrega, puede implementar un filtrado de spam complejo adicional (y específico del usuario) utilizando herramientas como SpamAssasin o el filtrado Bayesiano. Al reducir la afluencia de mensajes de spam obvios, estos filtros que requieren muchos recursos pueden hacer su trabajo de manera mucho más eficiente.

Conclusión

Combatir el spam a nivel de servidor es un juego desafiante a medida que los spammers se vuelven más creativos en el abuso de los mecanismos de los servidores de correo. Si su servidor aparece en la lista negra por spam de backscatter, debe tener cuidado con los escenarios de reenvío. Vigile las listas negras para ver si su servidor está causando problemas.

Bloquee los mensajes con códigos de error en lugar de devolverlos al remitente (rebotar). Configure el servidor con una política de entrega estricta. La mejor manera de prevenir el spam de backscatter es bloquear los mensajes antes de que entren al servidor de correo, ahora ya sabe cómo.