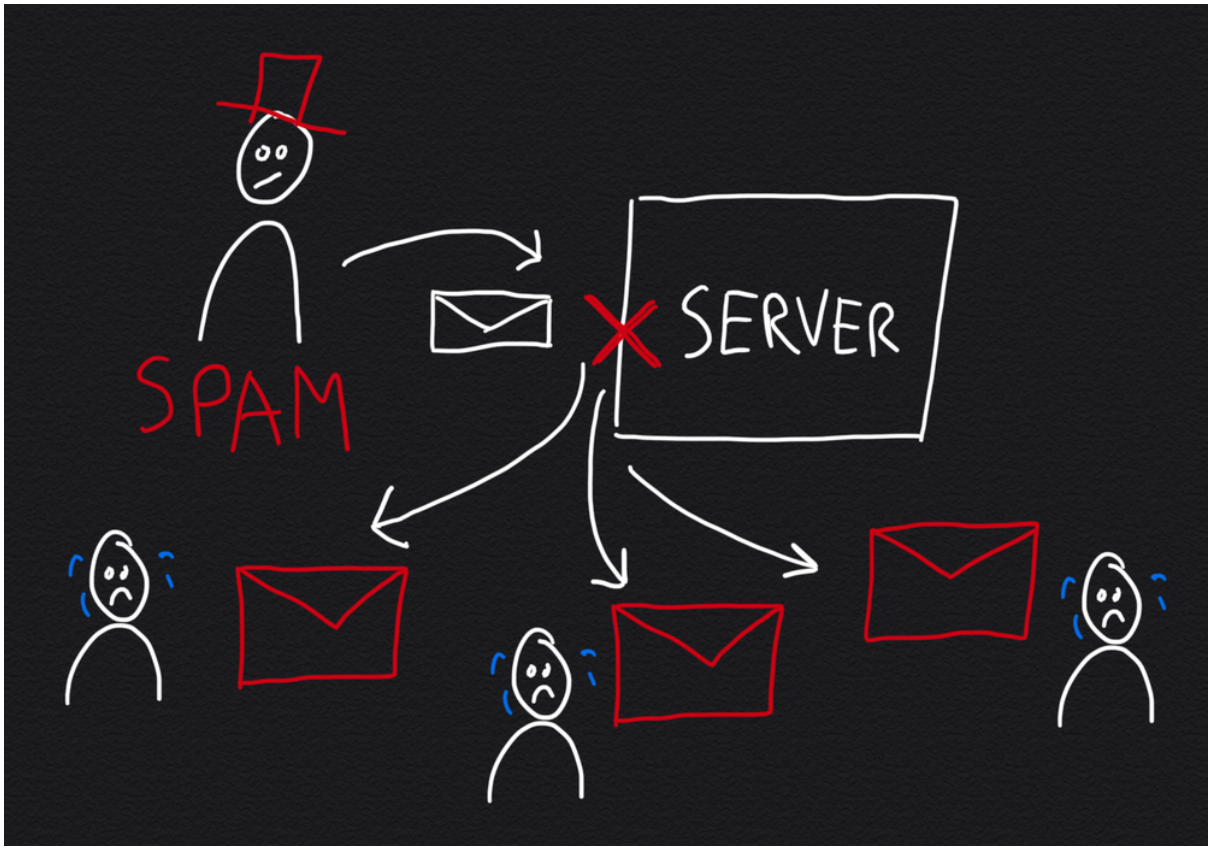
Backscatter spam op serverniveau bestrijden

Configureer Postfix om spam te blokkeren voordat het de server binnenkomt

Willem L. Middelkoop
10 sep. 2019



Deze maand had ik te maken met backscatter spam, wat effect had op één van de mailservers die ik beheer. Als server engineer zorg ik ervoor dat servers geen spam versturen en dat inkomende email gefilterd wordt. Ondanks alle inspanningen bleef deze server op de zwarte lijst komen te staan voor het versturen van spam naar iCloud, Office 365 en Google Gmail for Business (G Suite). Lees verder om erachter te komen wat de oorzaak hiervan was en hoe dit op te lossen.

Het probleem

De server is een Postfix mailserver op Debian GNU/Linux met alle laatste updates en beveiligingspatches. De server wordt gebruikt door legitieme klanten die deze alleen met

de juiste authenticatie kunnen gebruiken.

Voorkomen dat de server een open relay wordt

Individuele gebruikersauthenticatie op een mailserver is een belangrijke maatregel tegen misbruik van de mailserver. Als er spam wordt verzonden, kun je door te kijken naar de logs van de mailserver zien welke gebruiker het probleem veroorzaakt. In technische termen betekent dit dat je voorkomt dat de server 'een open relay' wordt. Postfix biedt veel instellingen om _SMTP_relay_met_behulp_van_toegangscontrole te beperken.

Snelheidsbeperking voor (gehackte) mailaccounts

Servermisbruik door individuele gebruikers gebeurt wanneer hun computer een virus krijgt of wanneer hun wachtwoord wordt onderschept. Dat kan gebeuren wanneer je je mail opent via een onveilige wifi zonder encryptie (TLS/SSL). Voor dergelijke situaties is het een goed idee om de hoeveelheid e-mails die individuele gebruikers mogen verzenden te beperken. Je kunt individuele Postfix configuratie parameters gebruiken (zoals *smtpd_client_message_rate_limit, smtpd_client_connection_rate_limit* en *smtpd_client_recipient_rate_limit*) of een Postfix firewall zoals Postwfd gebruiken.

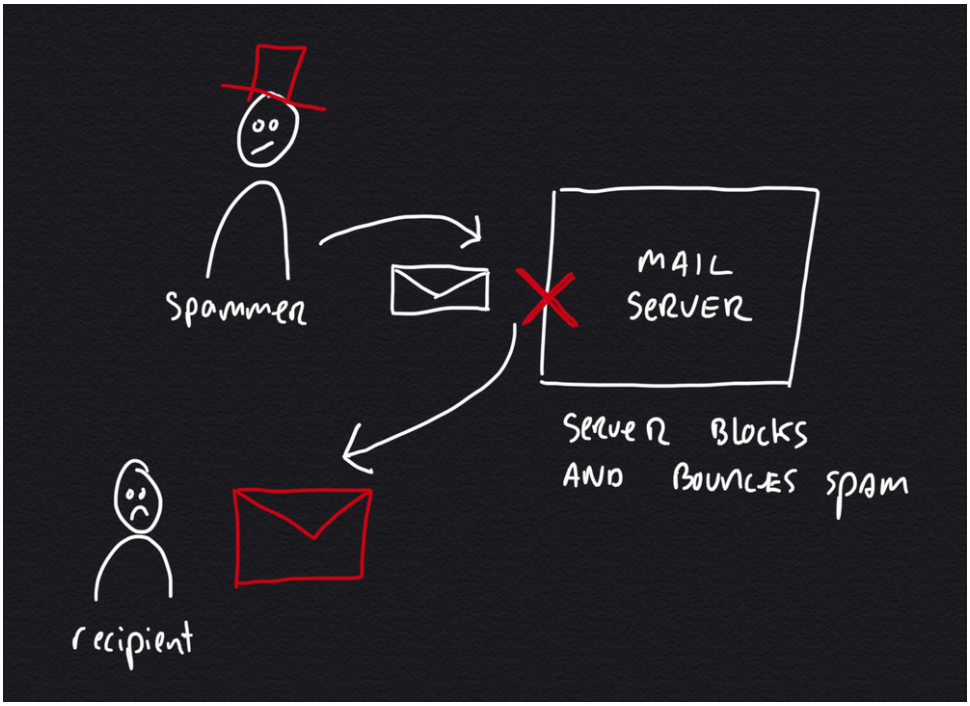
De server wordt vermeld op de zwarte lijst van 'backscatterer.org'

Ondanks alle maatregelen tegen spammisbruik, werd de server toch vermeld op `http://backscatter.org` voor het verzenden van spam. Als een server op een zwarte lijst wordt geplaatst, zullen andere servers deze niet langer vertrouwen en alle berichten als verdacht beschouwen. Dit kan ertoe leiden dat je (legitieme) berichten door andere servers als spam worden gezien (false positives). Om te begrijpen waarom dit is gebeurd, moet je eerst begrijpen wat backscatter spam is.

Wat is Backscatter spam?

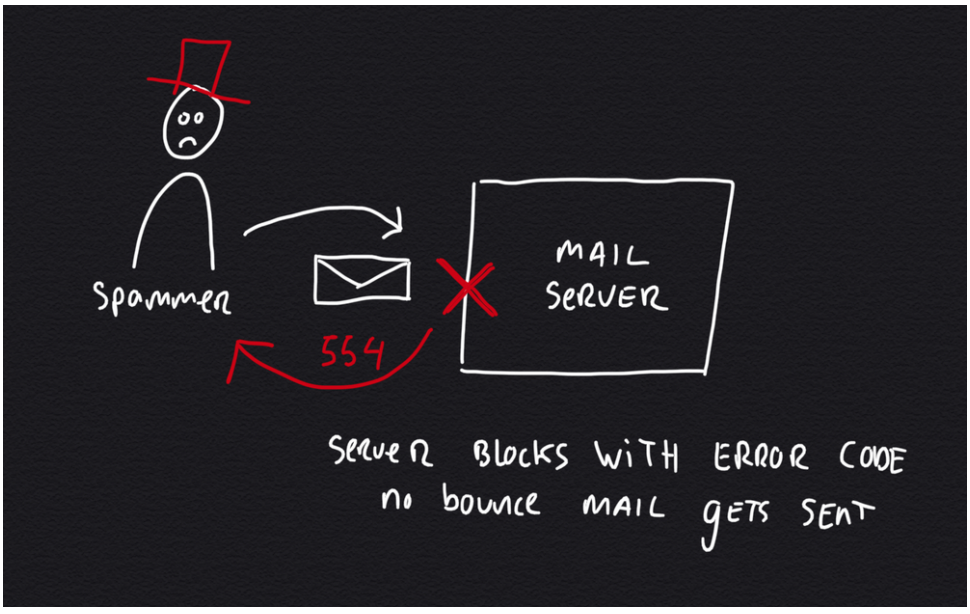
Backscatter spam zijn onjuist geautomatiseerde bounceberichten die door de mailserver worden verzonden, meestal als bijwerking van inkomende spam.

Backscatter treedt op wanneer spammers het afzenderadres vervalsen. Ze versturen een e-mailbericht waarvan ze verwachten dat het wordt gebounced met het adres van iemand anders als afzender. Wanneer het e-mailbericht bounced, retourneert de mailserver het bericht aan de vervalste afzender... waardoor de server in feite spam aflevert aan het afzenderadres.



Eenvoudig backscatter-scenario, mailserver stuurt bericht terug naar een vervalst afzenderadres

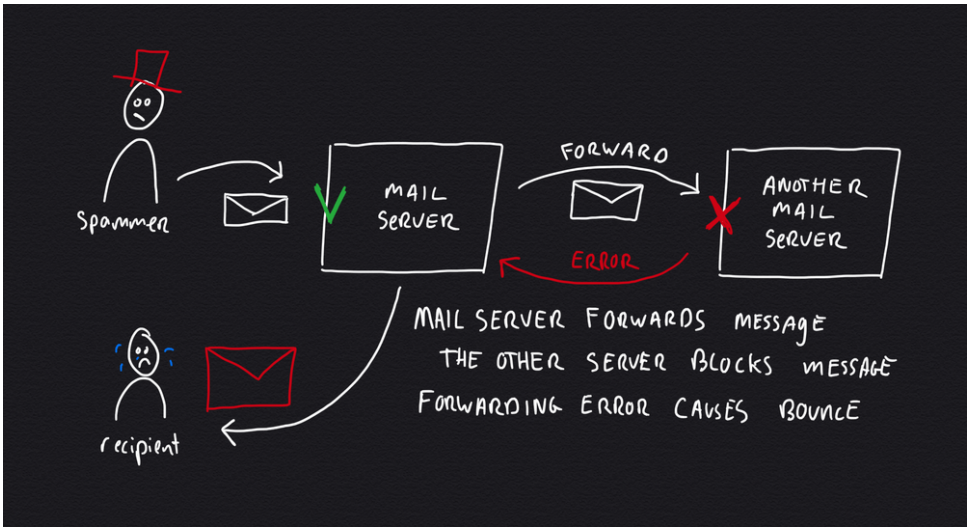
Het eenvoudige backscatter-scenario is waar een bericht wordt gebounced naar de verkeerde afzender. Het is een scenario dat eenvoudig op te lossen is door de server zo te configureren dat deze geen bounceberichten verzendt, maar in plaats daarvan reageert met een SMTP-foutcode.



Voorkom backscatter-bounceberichten door te reageren met SMTP-foutcodes

Helaas is er nog een (moeilijker) scenario waardoor je mailserver backscatter spam verzendt. Dit gebeurt wanneer iemand op je server zijn of haar mailaccount configureert om e-mail door te sturen naar een ander adres. De tweede server heeft mogelijk

een strenger spamfilter waardoor berichten bij het doorsturen worden geblokkeerd. Je mailserver zal dan de oorspronkelijke afzender informeren dat het doorsturen is mislukt, wat backscatter spam veroorzaakt.

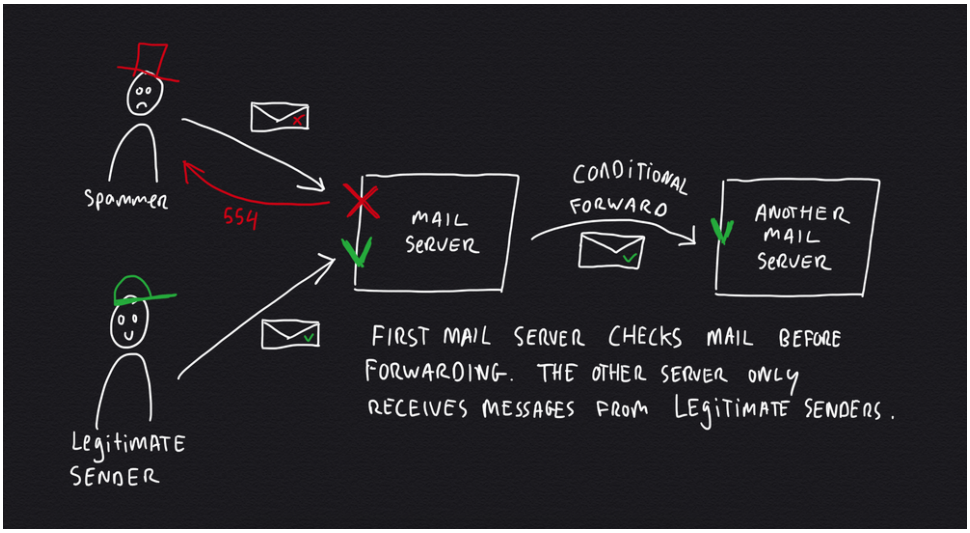


Veroorzaken van backscatter-spam wanneer de eerste mailserver e-mail doorstuurt naar een andere server die het bericht blokkeert

Het doorstuurscenario is veel moeilijker op te lossen, omdat je mogelijk geen controle hebt over de andere mailserver of de spamfilterinstellingen ervan. Wat nog erger is, is dat er vaak enige vertraging is tussen het accepteren van het bericht en het doorsturen ervan, waardoor het onmogelijk is om te wachten op een reactie van de andere mailserver.

Voorkom backscatter spam

De enige manier waarop je backscatter spam volledig kunt voorkomen, is door zeer streng te zijn bij de eerste mailserver, in de initiële SMTP-verbindingsfase. Dit lost het uitdagende 'doorstuurscenario' op door zeer selectief te zijn welke berichten worden doorgestuurd.



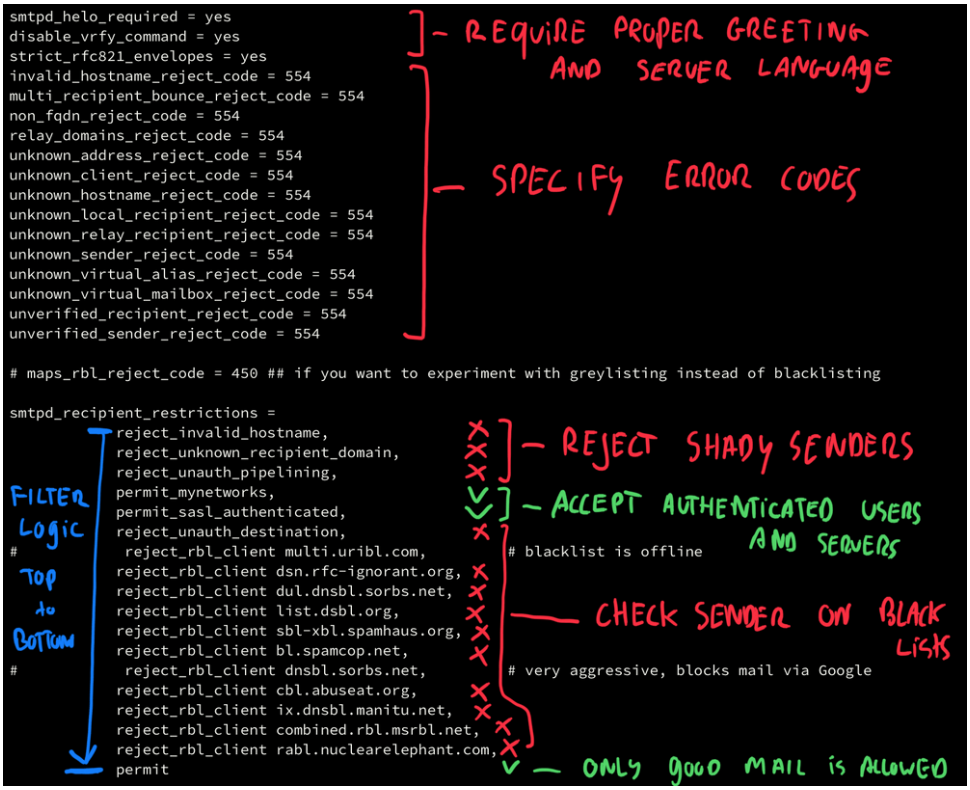
Voorkom backscatter-spam door alle berichten te controleren voordat u ze doorstuurt naar een andere server

Hoe spam te blokkeren voordat het de server binnenkomt

De beste manier om backscatter spam te voorkomen, is door deze te blokkeren voordat deze de (keten van) server(s) binnenkomt.

Traditioneel gebruiken servers geavanceerde spamfilters zoals SpamAssasin om berichten één voor één te analyseren. Dit veroorzaakt extra belasting op de mailserver.

Het is veel gemakkelijker om naar de afzender te kijken (bijv. of hij een rode hoed draagt) voor initiële filtering. Staat de afzender op een zwarte lijst? Gebruikt hij een 'normale' mail-app, of worden berichten verzonden door een virus of malware? Je kunt veel dingen bepalen door te kijken naar de 'taal' die de afzender spreekt.



Implementeren van strenge SMTP-beperkingen in Postfix - geannoteerde schermafbeelding van main.cf

In Postfix kun je SMTP-beperkingen opgeven in het configuratiebestand *main.cf*. Er zijn controles die kunnen worden gebruikt om berichten te blokkeren. Het is een goed idee om van 'gemakkelijk naar moeilijk' te werken in de filterlogica, beginnend met dingen die kunnen worden gecontroleerd zonder externe servers te raadplegen. Dit vermindert netwerkverkeer en belasting. Alleen als een bericht alle controles doorstaat, wordt het toegestaan voor bezorging (of doorsturen).

Bij bezorging kun je extra complexe (en gebruikersspecifieke) spamfiltering implementeren met behulp van tools zoals SpamAssasin of Bayes filtering. Door de instroom van voor de hand liggende spamberichten te verminderen, kunnen deze resource-intensieve filters hun werk veel efficiënter doen.

Conclusie

Het bestrijden van spam op serverniveau is een uitdagend spel, omdat spammers steeds creatiever worden in het misbruiken van mechanismen van mailservers. Als je server op de zwarte lijst komt te staan voor backscatter spam, moet je oppassen voor doorstuurscenario's. Houd zwarte lijsten in de gaten om te zien of je server problemen veroorzaakt.

Blokkeer berichten met foutcodes in plaats van ze terug te sturen naar de afzender (bouncen). Configureer de server met een strikt bezorgingsbeleid. De beste manier om backscatter spam te voorkomen, is door berichten te blokkeren voordat ze de mailserver binnenkomen, nu weet je hoe.