

Inhoud

1. Inleiding.....	1
2. Limieten.....	1
2.1 Deblokkeren.....	2
3. Veel voorkomende oorzaken.....	2
3.1 Open Relay mail server.....	2
3.2 Unauthorized mail.....	2
3.2.1 Non Delivery Reports.....	2
3.2.2 Instellingen testen.....	3
3.2.3 Lokaal domein.....	3
3.3 Virussen / spyware.....	3
3.4 Nieuwsbrieven.....	3

Wijzigingen

<i>datum</i>	<i>versie</i>	<i>auteur</i>	<i>wijziging</i>
23/08/2010	1.0	Timmo Verlaan	Creatie

1. Inleiding

Met de migratie naar het nieuwe mailplatform heeft UNET strikte limieten ingesteld om het versturen van SPAM en virussen tot een minimum te beperken. Met deze maatregelen verwachten we te voorkomen dat de SMTP servers van UNET op een blacklist geplaatst worden.

In dit document lichten we de gekozen limieten toe en beschrijven we welke acties ondernomen kunnen worden om te voorkomen dat de limieten overschreden worden.

2. Limieten

UNET hanteert voor het verzenden van e-mail via smtp.unet.nl limieten per IP adres, per dag. De grenzen zijn vastgesteld op basis van ervaring en type limiet. Afhankelijk van het type verwacht gebruik, worden er twee grenzen gehanteerd: Normaal en Groot verbruik. Voor vrijwel alle gebruikers is Normaal meer dan voldoende. Op ons totale klantenbestand heeft minder dan 3 % de Groot verbruik grens nodig.

Het is aan te raden van te voren te controleren hoeveel mail er per dag verstuurd wordt. U kunt dan voordat u via UNET mailt aangeven of u een Groot verbruik limiet wenst. Dit kan via een email, bij voorkeur met een indicatie van het mail volume en een (korte) toelichting. UNET zal vervolgens bepalen of u in aanmerking komt voor dit limiet.

	Normaal	Groot verbruik
E-mailberichten (per dag)	650	5.000
Geadresseerden (per dag)	2.000	15.000
Aantal geadresseerden (per bericht) ¹	50	50
Aantal onterechte bounces (per dag) ²	15	15
Aantal virussen (per dag)	15	15

¹ Het is niet mogelijk om een e-mailbericht te sturen naar meer dan 49 e-mailadressen. Een bericht met in totaal (to:, cc: en bcc:) meer dan 49 adressen wordt geweigerd door de mailserver.

² Het betreft hier bounce berichten die verstuurd worden door een mail server van de gebruiker. In het volgende hoofdstuk staat meer informatie over de achterliggende configuratie.

Zodra u een van de limieten overschrijdt, wordt uw IP adres automatisch geblokkeerd. U wordt zo spoedig mogelijk geïnformeerd over deze overschrijding.

2.1 Deblokkeren

Het deblokkeren van uw IP-adres op de SMTP server heeft een maximale doorlooptijd van 1 werkdag. U kunt een deblokkade aanvragen door een e-mail te sturen aan 'abuse@unet.nl'. Meldt hierin de oorzaak van het overschrijden van het limiet en de ondernomen actie die dit in de toekomst moet voorkomen. Indien er geen correcte actie ondernomen is kan dit het deblokkeren vertragen of er volgt opnieuw een blokkade. Een tweede blokkade wordt alleen opgeheven als er een aantoonbare oorzaak en oplossing bekend is.

3. Veel voorkomende oorzaken

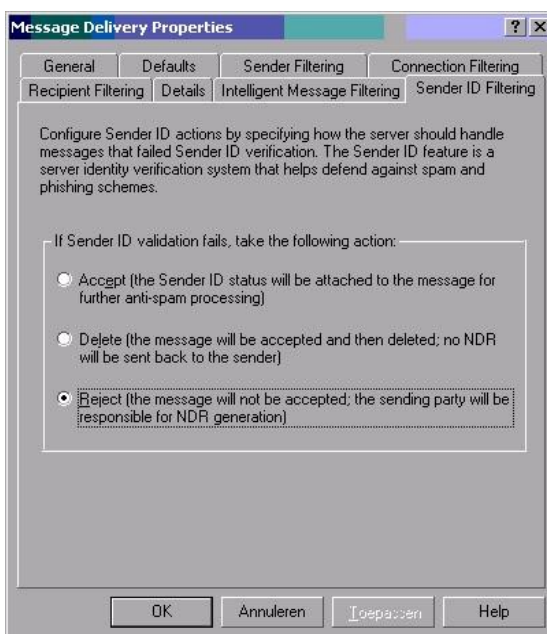
De limieten zijn ingesteld om onder meer het onderstaande gedrag van klanten en mailservers tegen te gaan. Onderstaand de meest voorkomende oorzaken van SPAM en de manier waarop ze weggenomen kunnen worden.

3.1 Open Relay mail server

Sommige mailservers hebben standaard in hun configuratie *Open Relay* aan staan. Dit betekent dat de server mail van iedereen zal accepteren en vervolgens gaan proberen die mail te versturen. Ideaal geschikt voor SPAMmers, die op zoek zijn naar mail servers om hun SPAM te bezorgen. En precies daarom ongewenst. Configureer mail servers altijd zo dat ze alleen e-mail doorsturen (relay) van een beperkt aantal IP adressen (bijv. alleen het LAN) of van bekende gebruikers. In vrijwel alle mailservers is dat eenvoudig te configureren.

3.2 Unauthorized mail

3.2.1 Non Delivery Reports



Een van de meest gebruikte manieren om SPAM te versturen is het proberen van zoveel mogelijk adressen bij een domeinnaam. De meeste van de adressen zullen daarbij niet bestaan. Een mailserver kan de berichten voor deze niet bestaande adressen op twee momenten weigeren: direct bij afdrukken van het bericht of bij het verwerken van het bericht. In het tweede geval wordt door de mailserver een bounce bericht gestuurd naar de verzender van het e-mailbericht. Precies dat bericht, een *non-delivery report*, wordt door veel mensen als SPAM ervaren.

Vandaar dat UNET vereist dat mailservers die mail aannemen het bericht direct bij afdrukken weigeren. De mailserver van de verzender zal dan zelf het bounce bericht voor de gebruiker maken.

Non Delivery Reports (NDR, bounces) komen alleen voor indien u een mailserver heeft. Deze mailserver ontvangt mail van bepaalde domeinen/adressen, maar controleert bij het afdrukken van de

berichten niet of het emailadres werkelijk bestaat.

De blokkering die ontstaat door een Bounce block, is alleen op te lossen door de NDR-instellingen aan te passen. Deze instelling moet op 'Reject' of 'Weigeren' staan.

3.2.2 Instellingen testen

U kunt de instelling van een mailserver eenvoudig testen. Log in via telnet op de betreffende mailserver (telnet [mailserver] 25). Voer vervolgens onderstaande stappen uit:

1. Typ "HELO *domein.tld*"
2. U krijgt een welkomstbericht vooraf gegaan door "250"
3. Typ "MAIL FROM: <>"
4. U krijgt het volgende bericht: "250 2.1.0 <>... Sender ok"
5. Typ "RCPT TO: *niet bestaand emailadres*"

Bij een correct geconfigureerde mailserver ziet u nu de foutmelding: "550 5.1.1 *emailadres*... No such user". Een voorbeeld:

```
telnet smtp.unet.nl 25
Connected to smtp.unet.nl.
Escape character is '^]'.
220-smtp.unet.nl ESMTP Exim 4.69 Fri, 18 Dec 2009 12:06:08 +0100
220- Sending spam or unsolicited commercial e-mail to this server is strictly
220- prohibited by our NO UBE / NO UCE policy. Abuse will be prosecuted and/or
220 charged per attempted recipient at international postal rates.
HELO domein.tld
250 smtp.unet.nl Hello domein.tld [IP-adres]
MAIL FROM: <>
250 OK
RCPT TO: nfo@unet.nl
550-Callout verification failed:
550-550 5.1.1 <nfo@unet.nl>: Recipient address rejected:
550 User unknown in local recipient table
RCPT TO: info@unet.nl
250 Accepted
```

3.2.3 Lokaal domein

Een andere oorzaak van de melding *Unauthorized mail* is het relay-en van als een mail server e-mail verstuurd vanaf een domein zonder correcte *reverse lookup*. Voor het domein zijn dan lokaal of in DNS wel de correcte MX verwijzingen opgenomen, maar de reverse lookup bij het IP adres verwijst niet terug naar dat domein. Vaak verwijst dat dan nog terug naar de standaard: *omgekeerd-IP-adres.bbserv.nl*.

De oplossing is om een correcte reverse DNS aan te laten maken. Maak eerst een A-record van een bestaand domein naar het IP-adres van uw mailserver. Vraag vervolgens een zogeheten PTR record aan met een verwijzing vanaf het IP adres naar het gewenste domein (bijvoorbeeld mail.uwdomein.nl). De DNS wijziging kan aangevraagd worden bij de UNET ServiceDesk en wordt alleen uitgevoerd als er een correct A-record aanwezig is.

3.3 Virussen / spyware

Indien u geen mailserver heeft (of die heeft uitgesloten als mogelijke oorzaak), dan wordt het versturen van SPAM vaak veroorzaakt door een virus of spyware op een desktop-computer. Daarom is het belangrijk dat u een virusscanner en firewall geïnstalleerd heeft om dit te voorkomen. Controleer deze computer daarnaast ook met enige regelmaat op spyware .

3.4 Nieuwsbrieven

Het versturen van een nieuwsbrief aan een groot adressenbestand kan betekenen dat u de limieten overschrijdt. Er zijn verschillende bedrijven die uw nieuwsbrieven op een professionele wijze kunnen verspreiden/verzorgen. Hiermee kunt u probleemloos nieuwsbrieven versturen, zonder rekening te houden met de SMTP limieten van UNET. Daarnaast helpen deze diensten u om te voldoen aan de [wetgeving over SPAM](#).