

MX-Relay configureren voor uw Office 365 omgeving

Configureren van MX-Relay

Het enige wat u hoeft te doen op ons platform is het domein aanmaken en vervolgens zorgen dat de berichten in uw Office 365 omgeving terecht komen. Dit doet u zo:

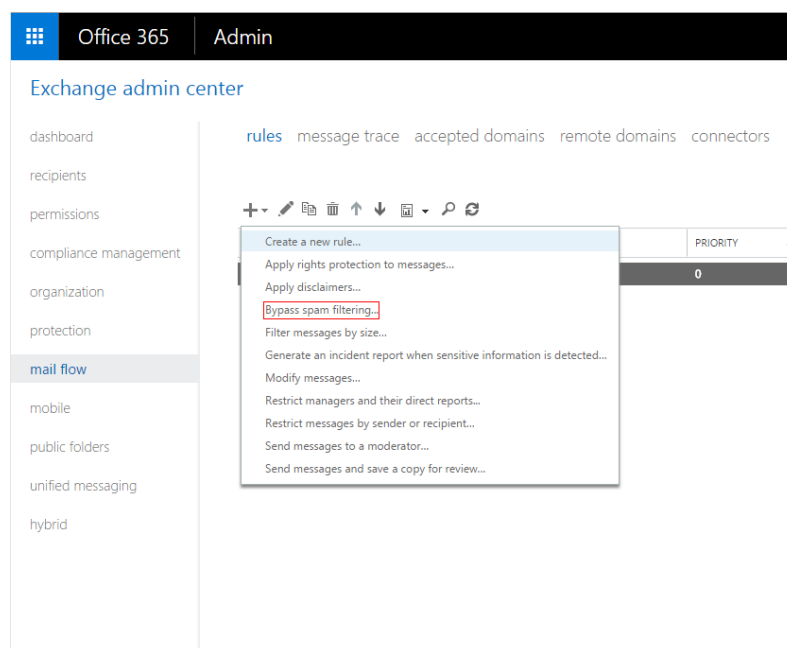
- 1) Voeg uw domein toe via onze portal website (zie www.mx-relay.com/faq als u niet weet hoe dit moet)
- 2) Log in op het filter waar uw domeinen op staan (bv. <https://cluster03a.mx-relay.com>)
- 3) Ga naar het zojuist aangemaakte domein en dan naar 'Basic', 'IP Instellingen'. Hier vult u uw outlook DNS naam in die je normaal gesproken zou gebruiken in uw MX record. Dus:
<domein>.mail.protection.outlook.com

Dat is eigenlijk alles wat u in de MX-Relay hoeft te doen

Configureren van Office 365

In uw Office 365 omgeving moeten nog wel enige zaken worden aangepast. Standaard zullen alle berichten die vanaf onze filters komen namelijk geblokkeerd gaan worden, omdat Microsoft oa. SPF checks doet. Deze gaan dan allemaal fout, want alle berichten komen nu immers vanaf onze IP nummers. Dus moet u onze IP nummers gaan uitsluiten van deze check. Dat doet u zo:

- 1) Log als admin in op uw Office 365 omgeving en ga naar Admin centers, Exchange.
- 2) Druk daarna in het linker scherm op 'mail flow' en ga dan naar 'rules'.
- 3) Druk op het '+' symbool en druk op 'Bypass spam filtering'.



4) Geef uw nieuwe rule een logische naam, bv. MX-Relay bypass.

5) Vervolgens gaat u naar 'Apply this rule if ...' en dan 'The sender ...' en dan 'IP address is in any of these ranges or exactly matches'.

new rule

Name:

*Apply this rule if...

Select one

Select one

The sender... is this person

The recipient... is external/internal

The subject or body... is a member of this group

Any attachment... address includes any of these words

Any recipient... address matches any of these text patterns

The message... is on a recipient's supervision list

The sender and the recipient... has specific properties including any of these words

The message properties... has specific properties matching these text patterns

A message header... has overridden the Policy Tip

[Apply to all messages] IP address is in any of these ranges or exactly matches

add exception domain is

Properties of this rule:

Audit this rule with severity level:

Not specified

Save Cancel

6) In het 'specify IP address ranges' scherm vult u vervolgens de IP nummers in van het MX-Relay cluster waar u op zit (zie eventueel www.mx-relay.com/faq voor al onze IP nummers).

specify IP address ranges

Enter an IPv4 address or range

209.222.80.0/21

64.235.144.0/20

OK Cancel

7) Druk vervolgens op 'Ok' en 'Save' om uw zojuist aangemaakte transport rule op te slaan en toe te passen.

8) Druk nu op het **Edit** icoontje bij deze nieuwe regel en ga naar de Eigenschappen van die regel. Stel het **Priority** veld in op '**0**'.

9) Sla als laatste op.

SMTP toegang alleen nog maar van onze servers accepteren (optioneel)

Standaard staat uw Office 365 omgeving SMTP (e-mail) toe vanaf heel het internet, dit is niet wenselijk want dan kunnen spammers nog altijd om ons filter heen mail afleveren op uw server.

Doorloop de volgende stappen om alleen nog mail verkeer toe te staan van onze IP nummers:

- 1) Log als admin in op uw Office 365 omgeving en ga naar Admin centers, Exchange.
- 2) Druk daarna in het linker scherm op 'mail flow' en ga dan naar 'rules'.
- 3) Druk op het '+' symbool en druk op 'Bypass spam filtering'.
- 4) Geef uw nieuwe rule een logische naam, bv. MX-Relay only.
- 5) Vervolgens gaat u naar 'Apply this rule if ...' en dan 'The sender ...' en dan 'Is External/Internal' en dan 'Outside the organization'.
- 6) Kies vervolgens vanuit het 'Do the following' drop-down menu de optie 'Reject this message with the explanation'. En vul vervolgens een melding in zoals bv. 'You have attempted to bypass our Email Security Service. Please ensure your DNS is up-to-date and try sending your message again.'
- 7) Scroll naar beneden en druk op 'Advanced Options' en druk op 'Add Exception'.
- 8) Selecteer dan 'The Sender', 'Sender's IP address is in any of these ranges or exactly matches'.
- 9) Vervolgens voegt u de IP nummers van ons cluster in en eventueel onze fallback server (zie: www.mx-relay.com/faq voor alle IP nummers van ons).
- 10) Scroll naar de **Eigenschappen** voor deze regel en stel het **Priority** veld op '**0**' in.
- 11) Ga naar **Match sender address in message** en selecteer **Envelope**.
- 12) In de nieuwe regel kiest u voor **Stop processing more rules** en druk daarna op **Save** om de nieuwe regel op te slaan.
- 13) Office 365 is nu zo geconfigureerd dat er alleen nog maar e-mail geaccepteerd wordt vanaf onze IP adressen.
- 14) Zorg ervoor dat deze nieuwe regel helemaal bovenin staat. Als dit niet zo is kunt u op het **Pijltje omhoog** knopje drukken om hem wel bovenin te zetten.

Mailflow testen vanaf ons filtercluster

U bent nu bijna klaar! Het is verstandig om nu even te kijken of ons filter ook echt mail af kan leveren in uw Office 365 omgeving. Dit doet u zo:

- 1) Log weer in op ons filtercluster.
- 2) Ga naar het betreffende domein.
- 3) Ga naar 'Basic', 'IP Instellingen'.
- 4) Vul een geldig mail adres in en save deze instelling.

Bestemmings Mail Server TCP/IP Instellingen

Bestemmings server: <domain>.mail.protection.outlook.com Bestemmings Poort: 25
Het IP adres of de server naam van de SMTP server en de TCP poort. Aanbevolen: 25

Geldig Test Email Adres: admin@<domain> **Test SMTP Connectie**

Gebruik MX Records: Ja Nee
Zet op ja als de bovenstaande 'Bestemmings Server' een domein is email naar het geschied.
Aangeraden: Nee

- 5) Druk nu op 'Test SMTP Connectie'.

Een nieuw venster zal nu openen, hierin kunt u zien of deze test succesvol was of niet. Mocht deze niet goed gaan, mail (mailto: support@mx-relay.com) of bel onze support 070 320 67 94.

MX Records aanpassen

Nu we zowel de MX-Relay- als de Office 365 omgeving ingesteld en getest hebben is de laatste stap de MX records van uw domein aanpassen. Deze stonde waarschijnlijk direct naar Office 365, maar moeten nu dus gaan wijzen naar onze systemen. Hieronder ziet u de juiste instelling voor elk systeem van ons (afhankelijk van welk systeem u gebruikt):

filter01

filter01.mx-relay.com met een prioriteit van 10
fallbackdt.mx-relay.com met een prioriteit van 50

cluster02

cluster02.mx-relay.com met een prioriteit van 10
fallbackdt.mx-relay.com met een prioriteit van 50

cluster03

cluster03a.mx-relay.com met een prioriteit van 10
cluster03b.mx-relay.com met een prioriteit van 10
fallbackdt.mx-relay.com met een prioriteit van 50

cluster04

cluster04a.mx-relay.com met een prioriteit van 10
cluster04b.mx-relay.com met een prioriteit van 10
fallbackdt.mx-relay.com met een prioriteit van 50