MX-Relay

Inbound e-mail configuratie

Inhoud

Firewall instellingen

Als er een firewall voor de mailserver staat, of u heeft in de mailserver de smtp toegang beperkt moet de volgende hostname worden vrijgegeven: **delivery.antispamcloud.com**

Als uw firewall het vrijgeven van een hostname niet ondersteund kunt u ook de IP's vrijgeven die op de onderstaande pagina staan:
https://documentation.n-able.com/spamexperts/userguide/Content/Appendix/hc-deliv-ips.htm

LET OP! Deze IP adressen kunnen in de toekomst wijzigen. Het vrijgeven op basis van de hostname heeft hierom de voorkeur.

Zorg er ook voor dat de firewall DNS-TCP poort 53 niet blokkeert (om te voorkomen dat u de UDP packet limit size bereikt).

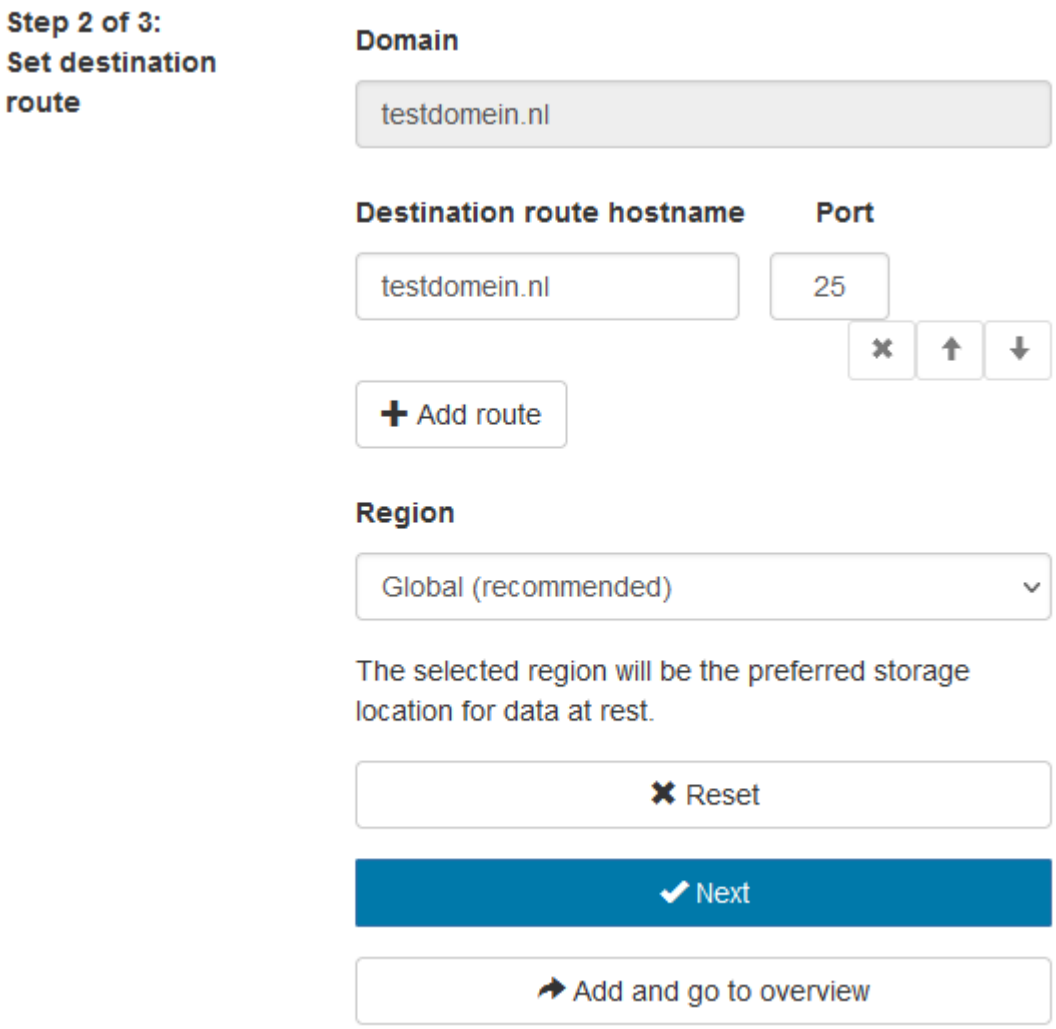
Als alternatief kan je op de mailserver een alternatieve poort instellen, zoals poort 2525 ipv de standaard 25. Deze poort kan in het spamfilter dan ook worden ingesteld

Domein toevoegen

1. Log in op ons control panel.
2. Ga naar 'General', 'Add domain'.
3. Vul hier het domein in (FQDN). Als je in één keer meerdere domeinen wilt toevoegen kan je dat doen door een CSV bestand te maken en hier te uploaden.

4. Klik op 'Continue'.

5. Op het volgende scherm kan je de FQDN (of het IP) van de MTA opgeven en tevens de te gebruiken poort.



6. Hier kan ook eventueel een 2e MTA opgegeven worden, deze wordt dan gebruikt als de eerste MTA niet bereikbaar is.
7. We raden aan de 'Region' op global te houden.
8. Klik op 'Next'.
9. In het volgende scherm wordt de connectie met de MTA getest (in het screenshot gaat dat niet goed uiteraard, omdat die domein naam niet bestaat).
10. Druk op 'Add and configure'.
11. In het configuratiescherm kan je eventueel nog instellingen aanpassen naar behoefte.
12. Klik op 'Save settings'.

De SMTP connectie controleren naar de mail server

Om te controleren of het spam filter mail kan afleveren op de mail server ga je in het beheer portaal naar Continuïty, Network tools en dan het tabblad SMTP. Hier kan je de hostname invullen van de mail server, dan een e-mail adres bij Envelope sender en Envelope recipient (dit moet een e-mail adres zijn binnen het domein dat je test). Dan klik je op Run en zie je of het goed gaat of niet. Als dit allemaal goed gegaan is kan je verder met het MX record wijzigen.

MX record wijzigen

Om te zorgen dat alle mail via het spam filter gaat maak je de volgende DNS wijzigingen aan in het MX record van het betreffende domein:

Prioriteit	MX record
10	filter10.antispamcloud.com
20	filter20.antispamcloud.com
30	filter30.antispamcloud.com
40	filter40.antispamcloud.com

Vanaf nu zal dan alle e-mail via het spam filter lopen.

O365 configuratie (deze stap kan je overslaan als je niet in O365 zit)

Als je gebruik maakt van de O365 cloud voor e-mail, moet je enkele stappen doorlopen om de mail flow vanaf ons spam filter mogelijk te maken.

Maak een partnerconnector en regel in Exchange Online om gefilterde e-mail te accepteren:

1. Meld u aan bij het Exchange-beheercentrum met beheerdersreferenties voor organisatiebeheer
2. Klik op 'Mail flow' > 'Connectors'.
3. Klik op de knop + om een connector toe te voegen
4. Kies het volgende:
   a. 'Connection from' – 'Partner organization'
   b. 'Connection to' – 'Office 365'.
5. Klik 'Next'.
6. Geef de connector een logische naam en geef eventueel een beschrijving op.
7. Zorg ervoor dat de instelling 'What do you want to do after connector is saved?' op '**Turn it on**' staat.
8. Klik 'Next'.
9. Kies bij 'How do you want Office 365 to identify your partner organization?' voor '**By verifying that the IP address of the sending server matches one of the following IP addresses, which belongs to your partner organization'**.
   a. Voeg de volgende bezorg-IP-reeksen één voor één toe en klik op het +-symbool:

      130.117.251.0/25
      185.201.16.0/22
      192.69.18.0/24
      208.70.90.0/24
      45.91.121.0/24
      45.93.148.0/24
      45.131.180.0/24
      45.140.132.0/24
      193.41.32.0/24
      185.225.27.0/24
      80.91.219.0/24
      188.190.113.0/24
      45.147.95.0/24
      46.229.240.0/24

87.236.163.0/24
188.190.112.0/24
192.69.19.0/24
208.70.91.0/24
185.209.51.0/24
185.218.226.0/24
199.115.117.7/32
46.165.223.16/32
94.75.244.176/32

LET OP! Deze IP adressen kunnen in de toekomst wijzigen. Via onderstaande link vind u de meest recente link met IP-adressen.
https://documentation.n-able.com/spamexperts/userguide/Content/Appendix/hc-deliv-ips.htm

10. Klik 'Next'.
11. Selecteer bij 'Security restrictions' voor '**Reject email messages if they aren't sent over TLS**'.
12. Klik 'Next'.
13. Controleer de instellingen en klik op 'Create connector'.
14. Klik op 'Done'.

Maak een regel in de Microsoft 365 Defender Security Portal aan:

1. Meld je aan bij de Microsoft 365 Defender-beveiligingsportal
2. Onder het gedeelte 'Email & Collaboration' (in het linker menu) kies je voor 'Policies & Rules'.
3. Klik op 'Threat Policies'.
4. Blader naar 'Rules' en selecteer 'Enhanced filtering'.
5. Selecteer nu de connector die we in de stappen hiervoor hebben aangemaakt.
6. Selecteer 'Skip these IP addresses':
    a. 130.117.251.0/25
    b. 185.201.16.0/22
    c. 199.115.117.7/32
    d. 46.165.223.16/32
    e. 94.75.244.176/32
7. Bij 'Apply to these users' selecteer je 'Apply to Entire Organization'.
8. Klik op 'Save'.