MX-Relay

Inbound e-mail configuration

Content

Firewall settings

If there is a firewall in front of the mail server, or you have restricted SMTP access in the mail server, the following IP (ranges) must be released:

130.117.251.0/25
185.201.16.0/24
185.201.17.0/24
185.201.18.0/24
185.201.19.0/24
46.165.223.16/32
62.138.14.204
69.64.57.149
94.75.244.176/32
199.115.117.7/32
213.163.65.6

Also make sure that the firewall is not blocking DNS-TCP port 53 (to prevent you from entering the UDP packet limit size reached).

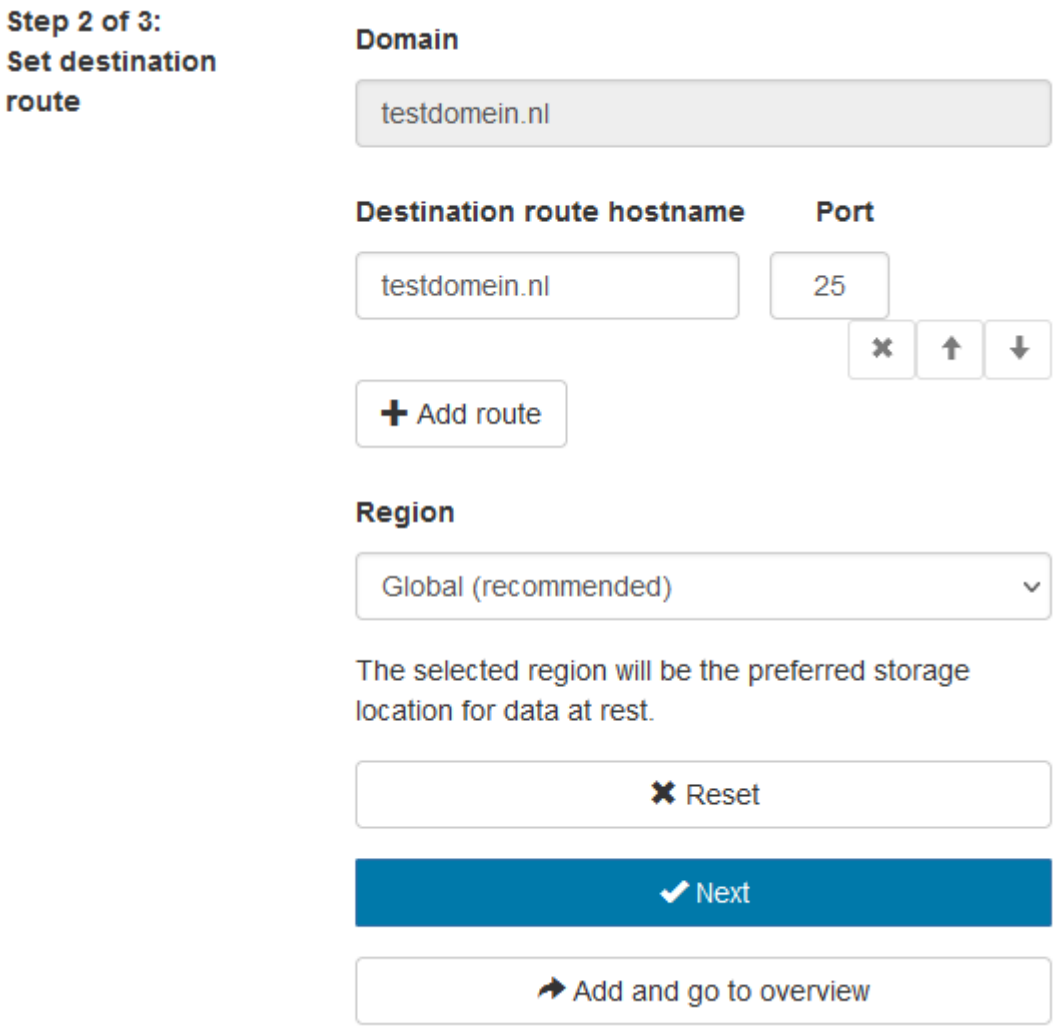
Alternatively, you can set an alternative port on the mail server, such as port 2525 instead of the standard port 25. This port can also be set in the spam filter.

Adding domains

1. Log in to our control panel.
2. Go to '**General'**, '**Add domain'**.
3. Enter the domain here (FQDN). If you want to add multiple domains at once you can do this by creating a CSV file and uploading it here.

4. Click on '**Continue'**.

5. On the next screen you can enter the FQDN (or IP) of the MTA and also the SMTP port.



6. A secondary MTA can also be specified here, which will then be used if the first MTA is not reachable.
7. We recommend keeping the '**Region**' set to **Global**.
8. Click on '**Next**'.
9. In the next screen the connection with the MTA is tested.
10. Press '**Add and configure**'.
11. In the control panel you can adjust settings according to your needs.
12. Click on '**Save settings**'.

Check the SMTP connection to the mail server

To check whether the spam filter can deliver mail to the mail server, go to the management portal to '**Continuity**', '**Network tools**' and then the '**SMTP**' tab. Here you can enter the hostname of the mail server, then an Envelope sender and Envelope recipient address (this must be an e-mail address within the domain you are testing). Then click on '**Run**' and see whether it goes well or not. If everything went well, you can continue to change the MX record.

Change MX record

To ensure that all mail goes through the spam filter, make the following DNS changes in the MX record of the domain in question:

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

From now on, all e-mail will go through the spam filter.

O365 configuration (you can skip this step if you are not in O365)

If you use the O365 cloud for email, you have to go through a few extra steps to receive the email flow from our spam filter.

Create a partner connector and rule in Exchange Online to accept filtered email:

1. Log in to the Exchange Admin Center with Organization Management admin credentials.
2. Click on '**Mail Flow > Connectors'.**
3. Click the **+** button to add a connector.
4. Choose the following:
    a. **Connection From** - **Partner organization**
    b. **Connection To** - **Microsoft 365**
5. Click **Next.**
6. Give the connector a **Name** you will recognize and optionally, provide a description.
7. Ensure the **What do you want to do after connector is saved** setting, **Turn it On** is selected.
8. Click **Next**.
9. Choose **By verifying that the IP address of the sending server matches one of the following IP addresses, which belong to your partner organization.**
10. Add the following delivery IP ranges one at a time and click the **+** symbol.
    - 130.117.251.9/25
    - 185.201.16.0/24
    - 185.201.17.0/24
    - 185.201.18.0/24
    - 185.201.19.0/24
    - 199.115.117.7/32
    - 46.165.223.16/32
    - 94.75.244.176/32
11. Click **next**.
12. Ensure that **Reject email messages if they aren't sent over TLS** is ticked and click **Next.**
13. Verify the settings and click **Create Connector**

14. Click **Done**.

Create the Rule in the Microsoft 365 Defender Security Portal

1. Login to the Microsoft 365 defender security portal with Organization Management admin credentials.
2. Under the **Email & Collaboration** section of the left-hand menu, select **Policies & Rules.**
3. Click **Threat Policies.**
4. Scroll to the **Rules** section and select **Enhanced Filtering.**
5. Select the Connector Name as created in the previous step.
6. Select **Skip these IP addresses**:
    1. 130.117.251.9/25
    2. 185.201.16.0/22
    3. 199.115.117.7/32
    4. 46.165.223.16/32
    5. 94.75.244.176/32
7. For **Apply to these users**, select **Apply to Entire Organization.**
8. Click **save**