MX-Relay

Migration Manual

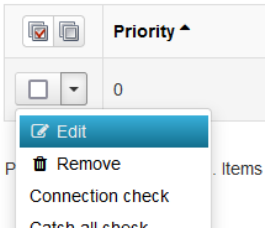
Content

Log in on the new spam filter

1. Log in to https://login.mx-relay.com
2. Go to ‘General’, ‘Domains overview’.

Here you will see all domains with the destination hosts (the mail servers). Check whether all domains are present and whether the destination hosts are set correctly. To change a destination host, do the following:

1. Click on the relevant domain.
2. Go to 'Incoming', 'Destinations'.
3. Now press the pull-down and choose 'Edit'.



4. In the new window you can adjust the priority, the host and, if necessary, the SMTP port. You only use priority if you have multiple mail servers.

Adjust firewall

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.

SMTP test

If all this is correct, you can continue with the SMTP test.

1. Go to 'Continuity', 'Network tools'.
2. Go to the 'SMTP' tab.

3. Enter the 'Hostname' (the destination host) plus a valid envelope sender and envelope recipient address.
4. Press 'Run' and see if the connection can be established successfully.

If all went well, you can adjust the MX records to the new anti-spam filter;

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 via the new spamfilter.

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

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

Create a partner connector and arrange Exchange Online to accept filtered email.

Creating a partner connector is done as following;

1. Sign in to the Exchange admin center with administrative credentials.
2. Click **Mail Flow > Connectors**.
3. Click the **+** button to add a connector.
4. Select the following: a. **Connection of – Partner organization** b. **Connect to - Microsoft 365**.
5. Click **Next**.
6. Give the connector a name you recognize and optionally provide a description.
7. Make sure the **What do you want to do after the connector is saved** setting is **Enable** is selected.
8. Click **Next**.
9. Choose **By verifying that the sending server's IP address matches one from the following IP addresses, which belong to your partner organization**.
   a. Add the following MX-Relay delivery IP ranges one by one and click on the **+** symbol:
   i. 130.117.251.0/25
   ii. 185.201.16.0/24
   iii. 185.201.17.0/24
   iv. 185.201.18.0/24
   v. 185.201.19.0/24
   vi. 199.115.117.7/32
   vii. 46.165.223.16/32
   viii. 94.75.244.176/32
10. Click **Next**.
11. Make sure that **Reject emails if not sent via TLS** is checked and click **Next**.
12. Check the settings and click **Create Connector**.
13. Click **Done**.

Create a rule in the Microsoft 365 Defender Security Portal:

1. Sign in to the Microsoft 365 Defender security portal with administrative credentials organizational management.

2. Under the **Email & Collaboration** section of the left menu, select **Policies & Rules**.
3. Click **Threat Policy**.
4. Scroll to the **Rules** section and select **Enhanced Filtering**.
5. Give the connector a name you recognize.
6. Select 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. For **Apply to these users**, select **Apply to entire organization**.
8. Click **Save**.

See also our other manuals in the knowledge base.