Securing the mails delivery

To secure your mail server and the delivery of your e-mails, we recommend that you use the following three protocols:

SPF

The Sender Policy Framework (SPF) allows to declare your mail server as authorized to originate mail for your domain(s).

To configure it, you have to add a single dns record:

Type: `TXT`
Host: `@` (depending of your DNS provider, it can be your domain name `example.com`, a blank string, a `@`, etc.)
Value: `v=spf1 include:_spf.hosterra.tech ~all`

DKIM

DomainKeys Identified Mail (DKIM) is an e-mail authentication method designed to combat mail spoofing.

To configure it, you have to add two dns records. To get these two specific records, just access the Plesk interface of your server, then:

1. click, in the left side menu, on **Mail**;
2. click the **Mail Settings** tab;
3. check the **Use DKIM spam protection system[...]** at the bottom of the page;
4. get the 2 dns records to add by clicking on **How to configure external DNS**.

DMARC

Once SPF and DKIM are configured and operational, you can set Domain-based Message Authentication, Reporting and Conformance (DMARC), a standard email authentication protocol by just adding one more dns record:

Type: `TXT`
Host: `_dmarc`
Value: `v=DMARC1; p=reject; pct=100`

> If you configure DMARC before configuring and validating both SPF and DKIM, you will be unable to correctly send emails from your server.

Testing you configuration

To test your SPF + DKIM + DMARC configuration, you can uses tools like:

- Red Sift's Investigate tool
- M@ilGenius
- Mail-Tester

Revision #12
Created 3 November 2023 10:32:26 by Pierre Lannoy
Updated 6 November 2023 15:04:48 by Pierre Lannoy