Mail-Server aufsetzen und dabei Klippen umschiffen

GPN23 – JENS DORFMÜLLER

Image by Gerralt van Soest from Pixabay

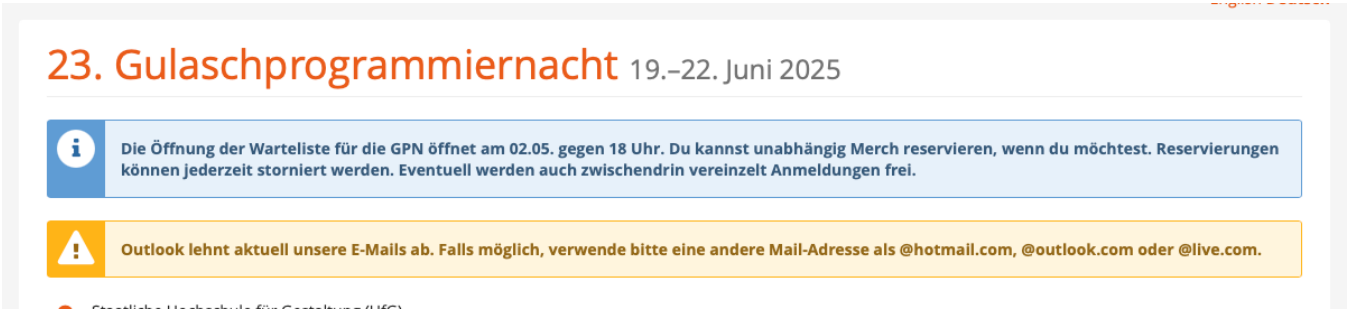
Einleitung Motivation

Person
- Jens Dorfmüller
- Hobby: Cosplaying as a Sysadmin

Historie
- Rund um die Jahrtausendwende: Mailserver an der Uni betrieben
- Danach: Mail-Accounts bei meinem Web-Hoster und die Mail-Exchange (MX) Records meiner Domains im DNS-System auf deren Mail-Server umgeleitet
- Vor ein paar Jahren: „mit Docker kann ich den Mailserver auch wieder selber betreiben!“

Projekt Mailu (https://mailu.io)
- Einfach zu benutzen
- inzwischen habe ich selber zwei Patches beigetragen

aber:
- Mail-Server zum Laufen bringen reicht nicht mehr!
- Man muss ständig auf seine Reputation achten!
- … und manchmal reicht selbst das nicht …



Hetzner-Server anlegen

HETZNER
Affiliate Link

Link: https://console.hetzner.cloud/

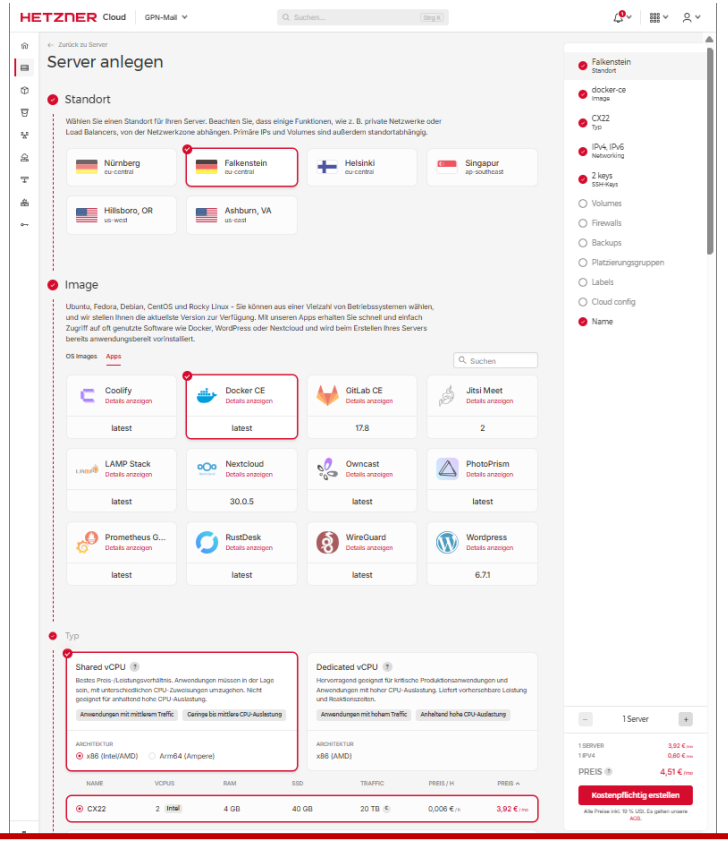
Login + evtl. neues Projekt anlegen

Ressource erstellen → Servers

Einstellungen in der Maske:

- Standort: z.B. Falkenstein
- Image: Apps → Docker CE
- Typ: Shared vCPU → x86 (Intel/AMD) → CX22 (4 GB RAM!)
- Networking: min. „Öffentliche IPv4“
- SSH-Keys: optional (sonst kommt root-Passwort per Mail)
- Name: z.B. gpn-mail-server

→ Kostenpflichtig erstellen (4,51€/Monat)



Post Scriptum:
Hetzer schränkt die Nutzung von Port 25 und 465 ein. Ihr müsst zusätzlich noch die Freischaltung beantragen (siehe FAQ).

Stopp: erst einmal IP-Adresse überprüfen

Wenn eine IP-Adresse früher einmal zum Versenden von Spam verwendet wurde, ist es viel Arbeit für seinen Mail-Server einen guten Ruf zu bekommen.

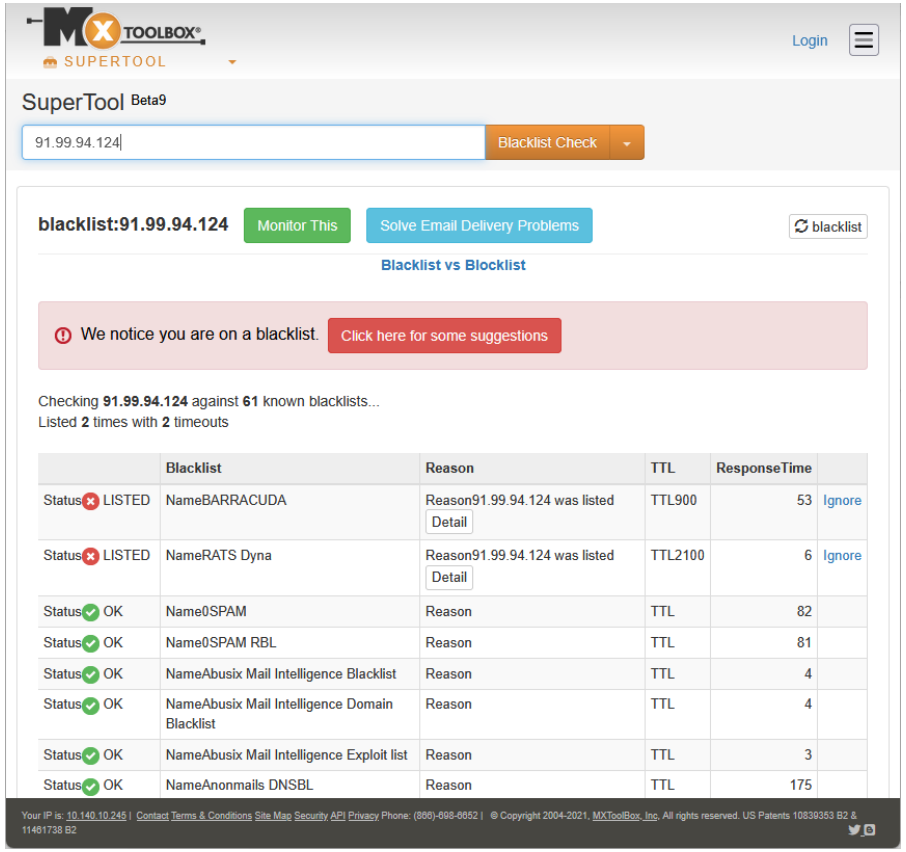
Checker finden über Google-Suche:
„mail ip blacklist check“

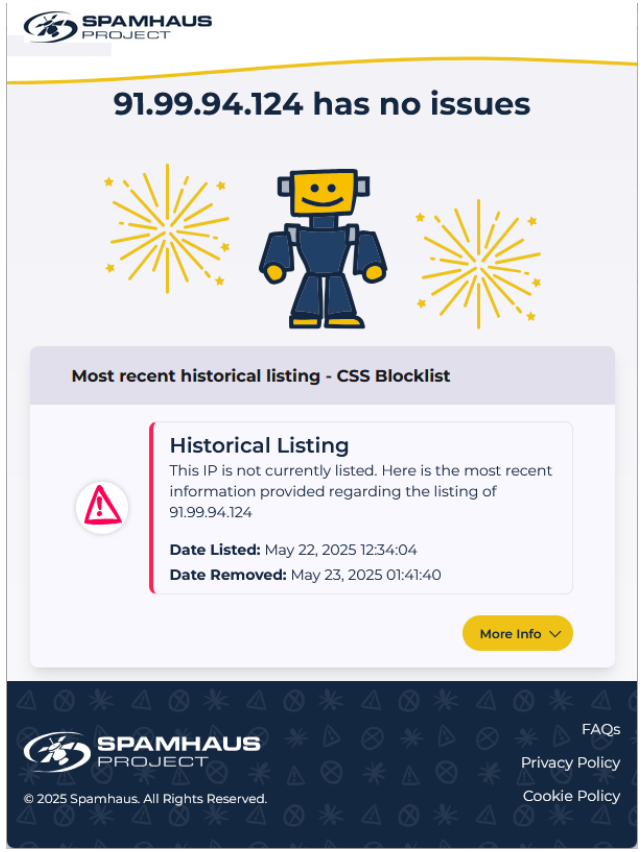
z.B.

- https://mxtoolbox.com/blacklists.aspx
- https://check.spamhaus.org/

→ Eine etablierte Mail-IP sollte man nicht leichtfertig abgeben/wechseln!

Mögliche Ergebnisse aus dem IP-Check





DNS-Einträge bei Hetzner

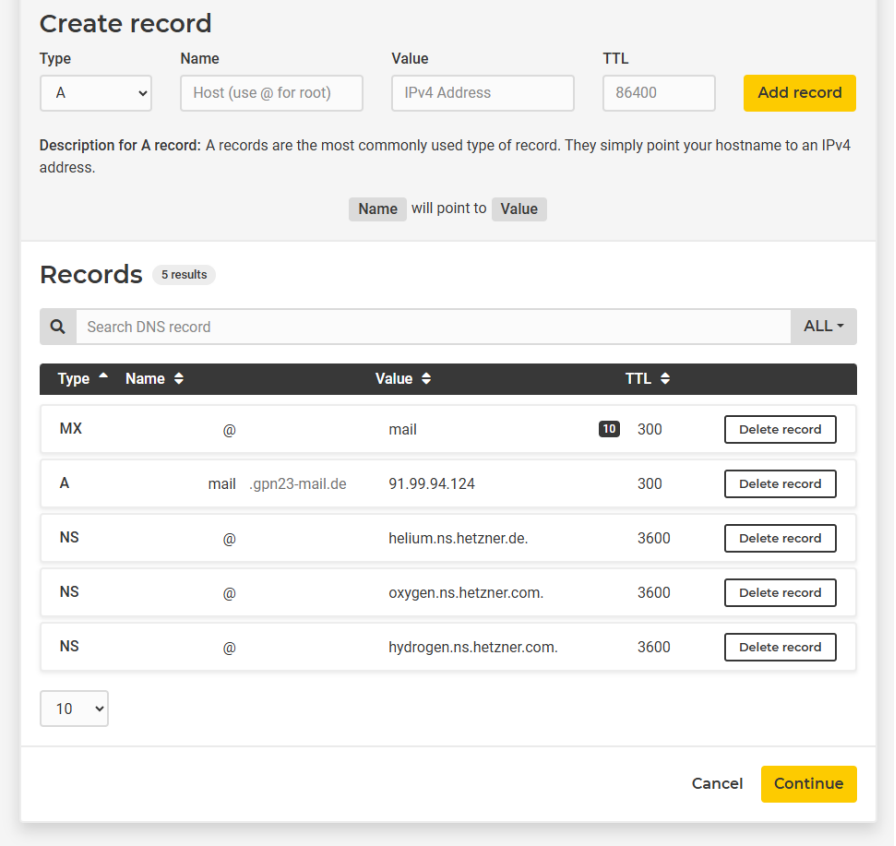
Hetzner DNS-Console:
https://dns.hetzner.com/

Notwendige Einträge:

- A-Record für mail-Server:
  z.B. mail.gpn23-mail.de → <IP Adresse>
- MX-Record für Domain:
  z.B.
  - Priority 10
  - @ → mail (= mail.gpn23-mail.de.)

Verteilung an DNS-Server dauert eventuell etwas

Kurze TTL erleichtert zu Anfang Fehlerkorrektur



Reverse DNS bearbeiten

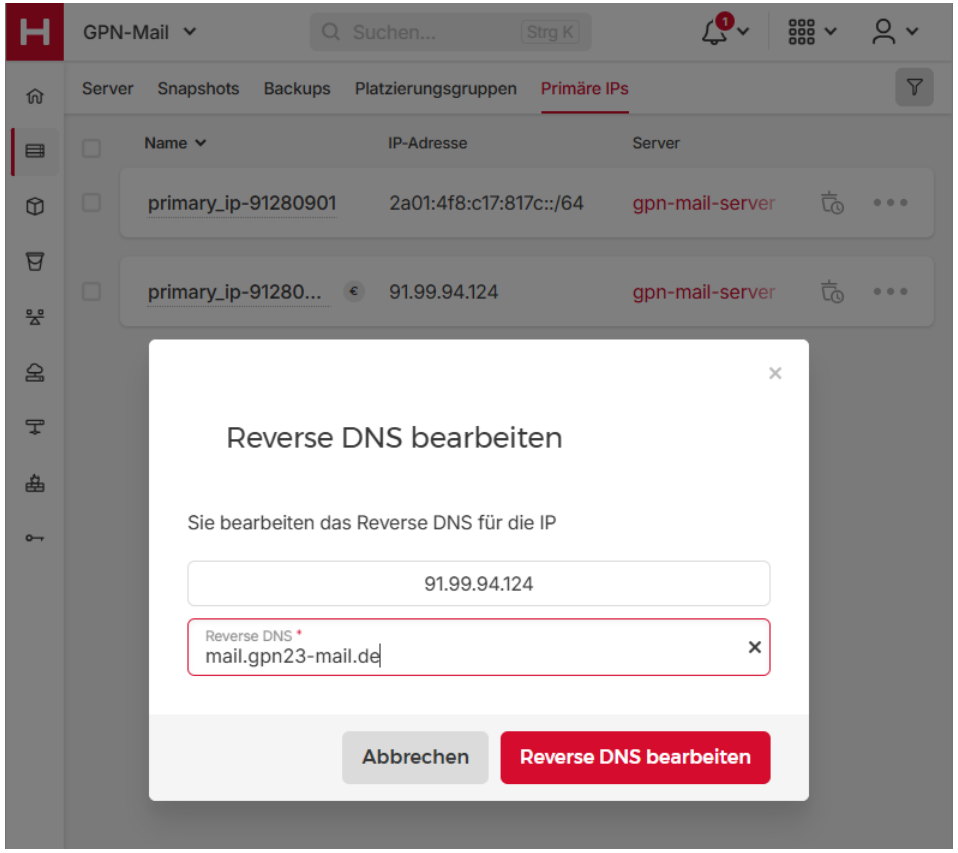
Mailu-Doku:
„With incorrect **reverse** DNS setup, most mail systems will reject your emails as spam.”

Hetzner-Cloud-Console

Server → Primäre IPs

Auf die drei Punkte rechts neben der IPv4-Adresse klicken

Reverse DNS eintragen:
z.B. mail.gpn23-mail.de



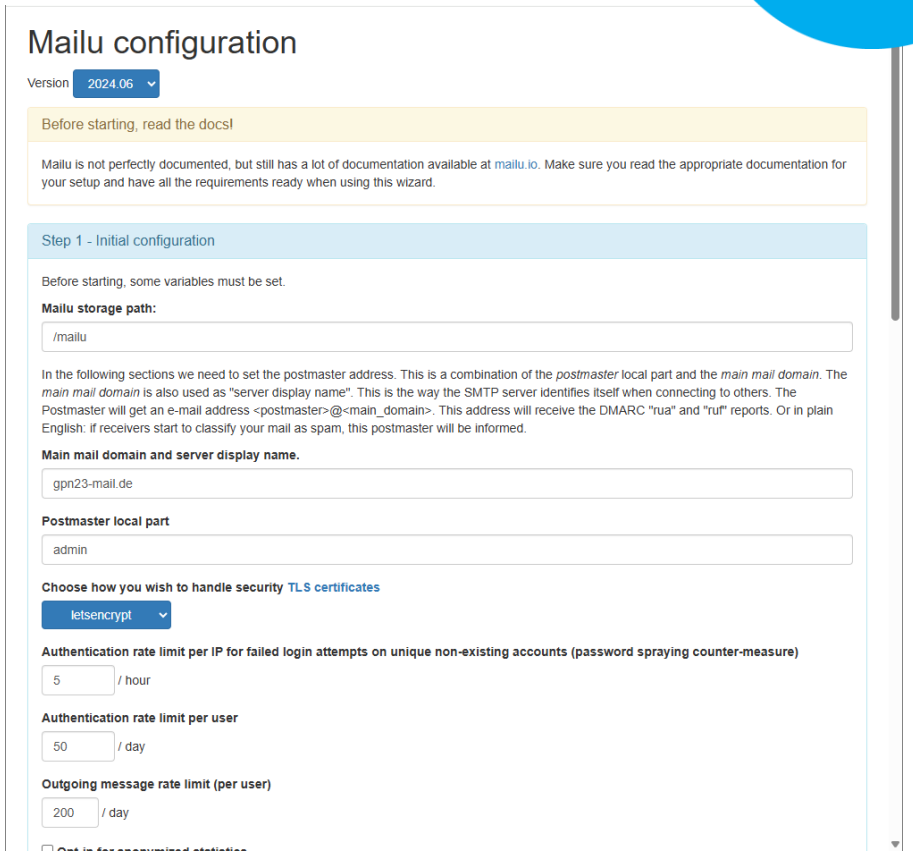
Config erstellen

Link: https://setup.mailu.io/2024.06/

Daten eintragen

- Main mail domain: z.B. gpn23-mail.de
- Website name: z.B. GPN23-Mailu
- Linked Website URL: z.B. https://gulas.ch
- Enable Web email client: roundcube
- Enable the antivirus service: yes
- Enable oletools: yes
- IPv4 listen address: <Server IP Adresse>
- Public hostnames: mail.gpn23-mail.de

→ Setup Mailu



Config übertragen und Docker starten

Login auf den Mail-Server:
`ssh root@mail.gpn23-mail.de`
(oder: `ssh root@<IP Adresse>`)

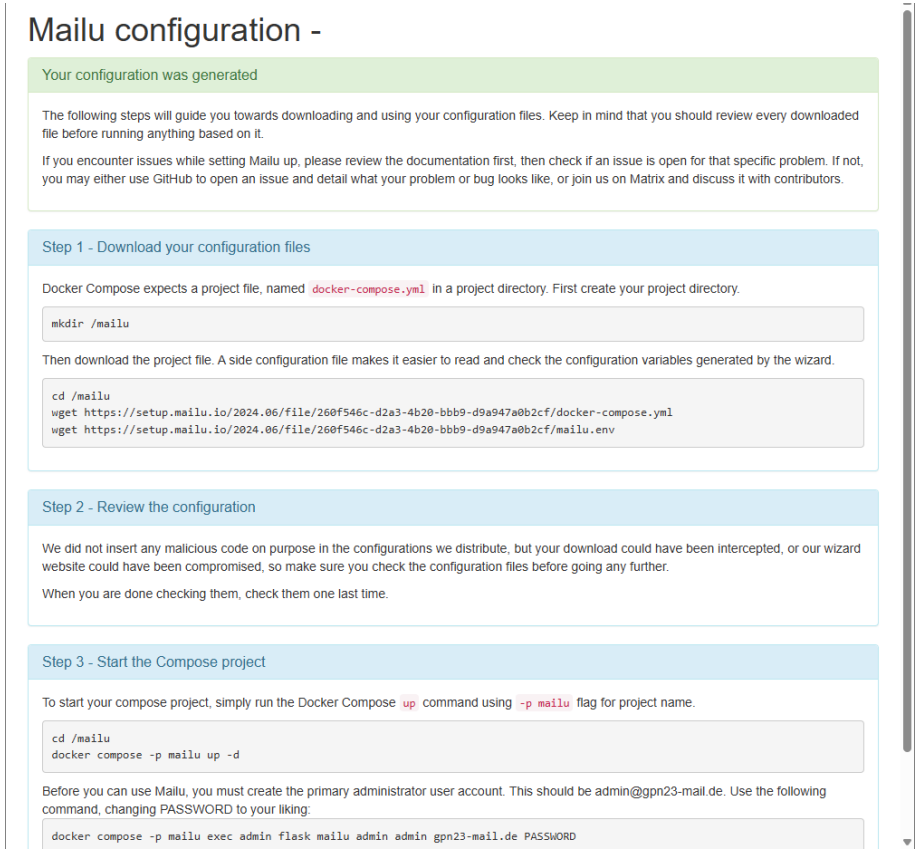
Server auf den neuesten Stand bringen
`apt update && apt upgrade`

Verzeichnis erstellen:
```
mkdir /mailu
cd /mailu
```

Per `wget` die Mailu-Config holen
(siehe rechts)

Mailu starten:
`docker compose -p mailu up -d`

Admin-Passwort setzen:
`docker compose -p mailu exec admin flask mailu admin admin gpn23-mail.de <PASSWORD>`



Admin Interface

Aufrufen des Web-Interfaces:
z.B. https://mail.gpn23-mail.de

Login als admin:

- Username: z.B. admin@gpn23-mail.de
- Password: <PASSWORD>

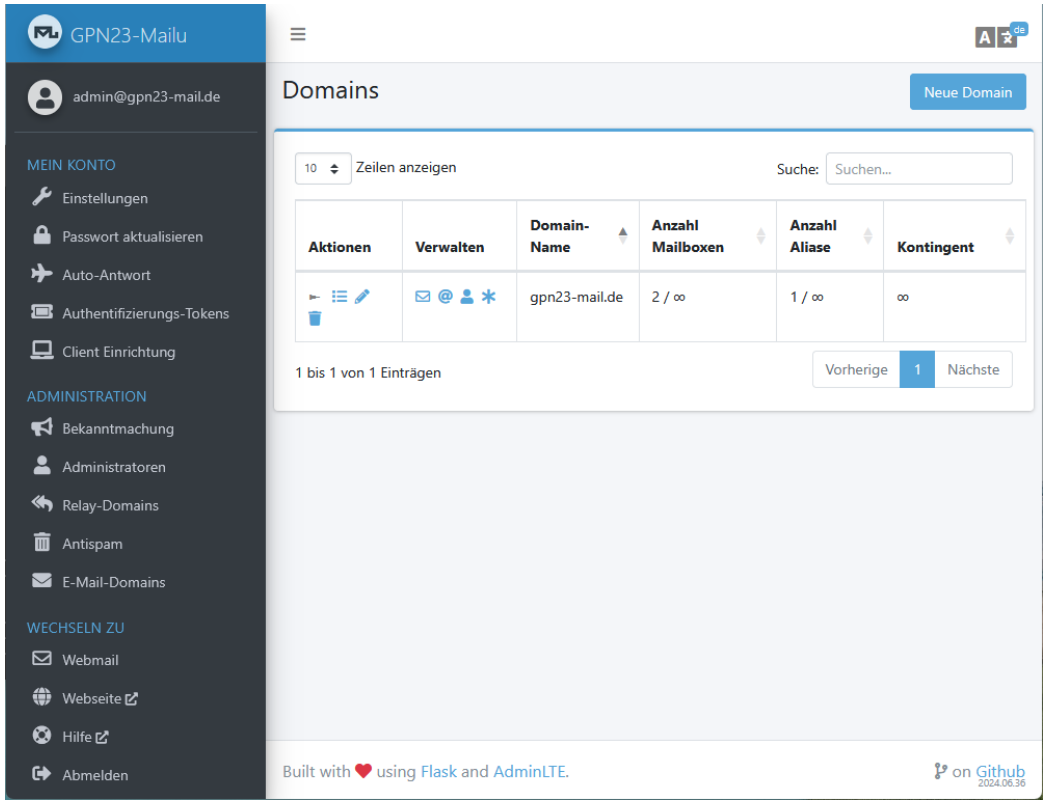
→ Anmelden Admin

IMAP + SMPT Server-Informationen: Mein Konto → Client Einrichtung

Neuen Account anlegen: Administration → E-Mail-Domains → Spalte: Verwalten → ✉ (Benutzer)

Neuen Alias anlegen:
Administration → E-Mail-Domains → Spalte: Verwalten → @ (Aliase) z.B. postmaster@gpn23-mail.de

Webmail: Wechseln zu → Webmail
(evtl. Server-Neustart notwendig:
docker compose down + docker compose up –d)



Webmail

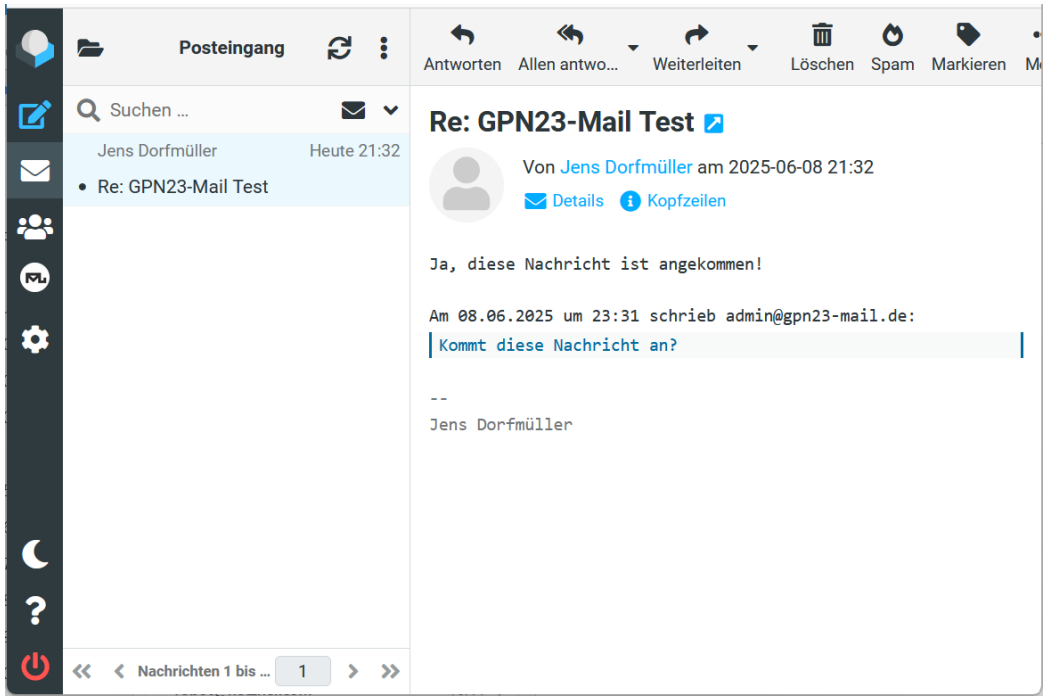
Ausprobieren:

- E-Mail versenden (an eigene Mail Adresse)
- E-Mail empfangen (einfach reply nutzen)

=> scheint alles zu funktionieren

Achtung: der Schein trügt!

Mein Mail-Server ist genügsam!



Stopp: SPF, DKIM, DMARC

Bild „Spam wall“ by freezelight, auf Flickr

Spam hat in den letzten in den letzten Jahrzehnten dazu geführt, große Anbieter kaum mehr anderen Mail-Servern blind trauen!

Maßnahmen:

SPF: Sender Policy Framework

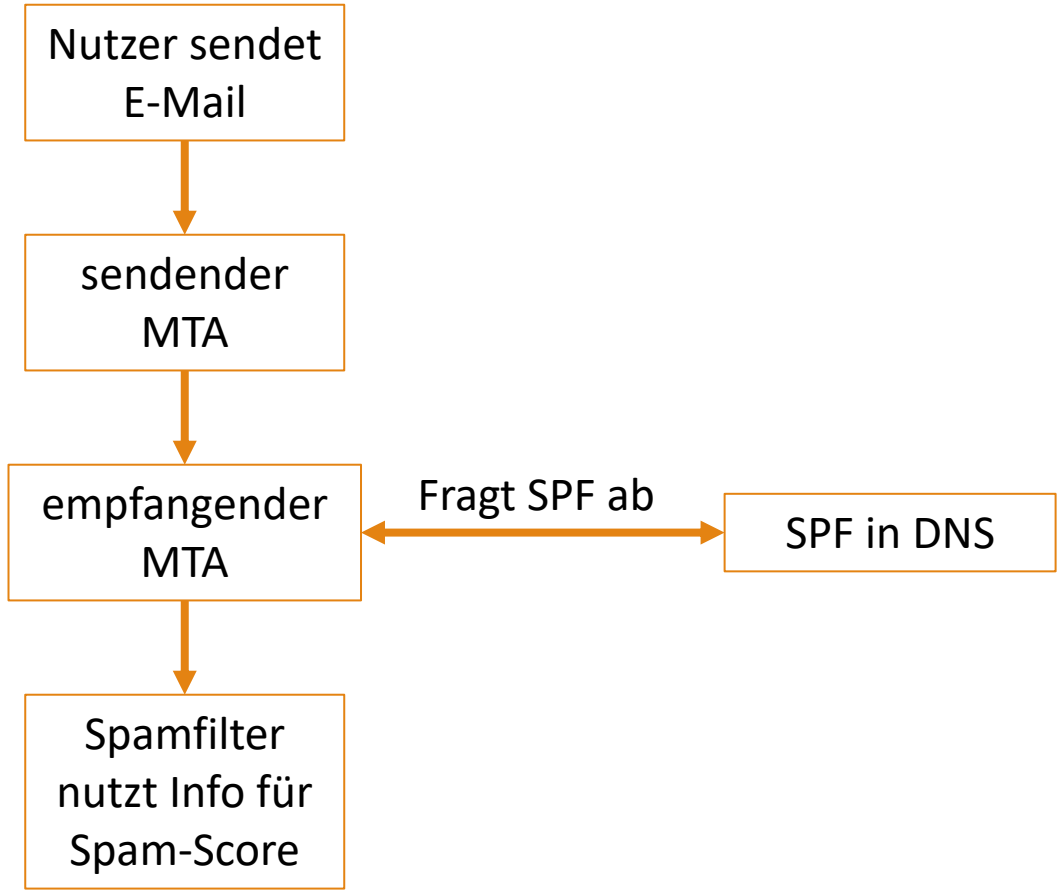
DKIM: DomainKeys Identified Mail

DMARC: Domain-based Message Authentication, Reporting and Conformance

Sender Policy Framework (SPF)

RFC 7208 (2014)

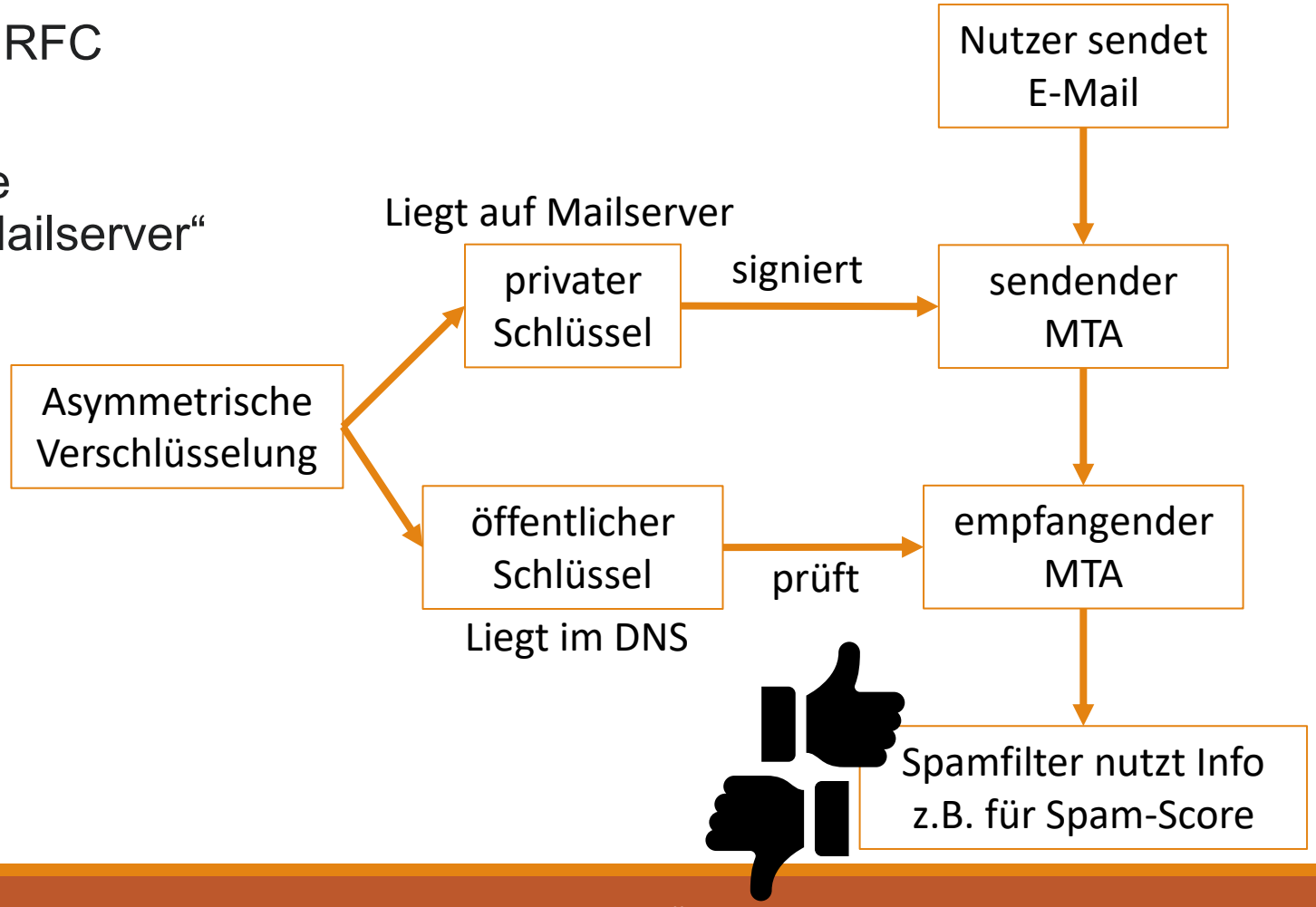
Empfangender Mail-Server:
„Ich habe e-mail von IP xy im Namen einer Domain bekommen! Darf diese IP überhaupt E-Mails für diese Domain verschicken?“



DomainKeys Identified Mail (DKIM)

RFC 6376 (2011) with updates in RFC 8301 and RFC 8463

„Mail stammt in bestimmter Weise unverändert vom absendenden Mailserver“



Signatur wird intern durchgeführt von:

RSPAMD
spam filtering system

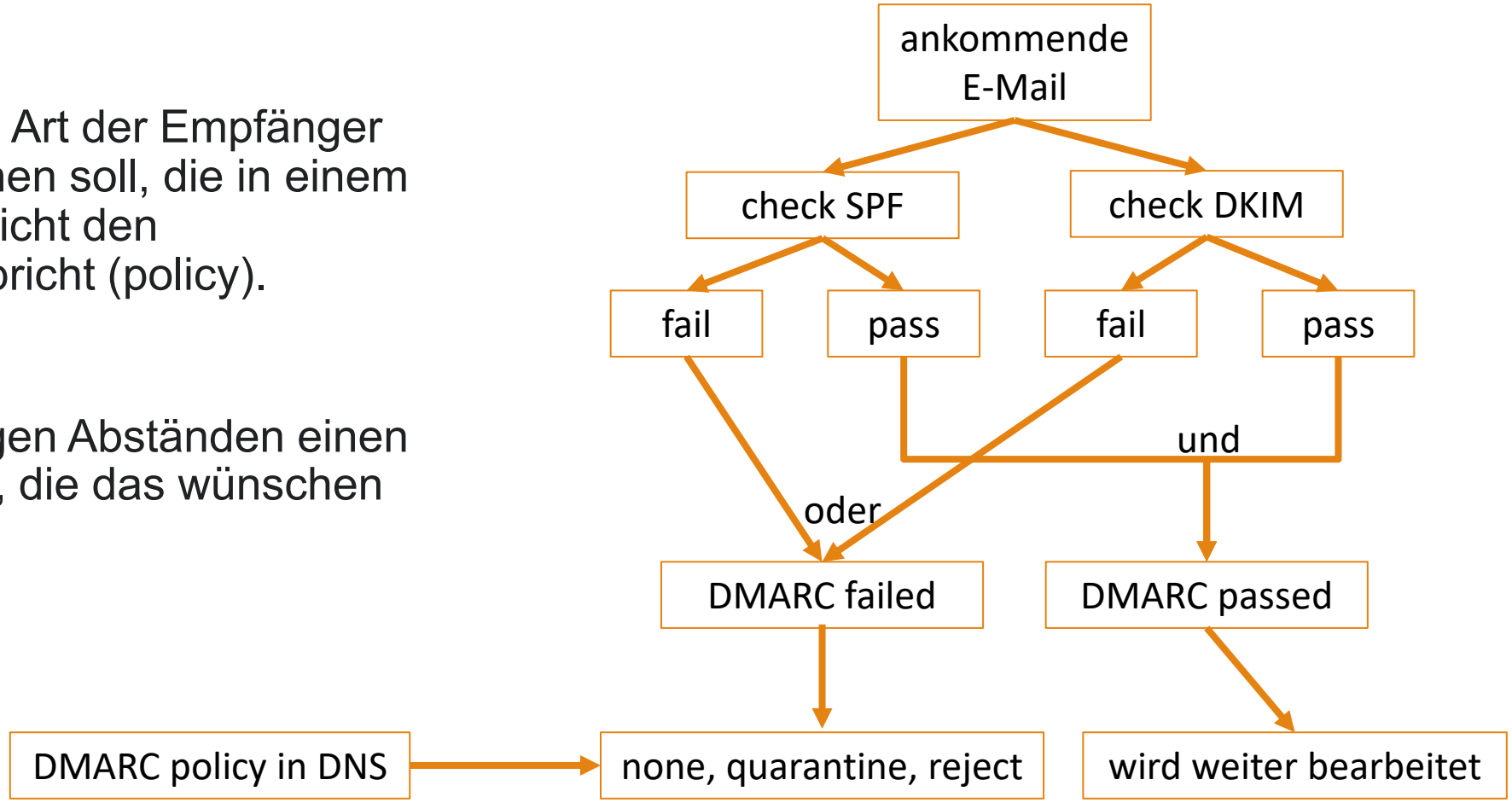
Domain-based Message Authentication, Reporting and Conformance (DMARC)

RFC 7489 (2015)

Legt fest, auf welche Art der Empfänger mit einer Mail umgehen soll, die in einem oder beiden Fällen nicht den Anforderungen entspricht (policy).

+

Sendet in regemäßigen Abständen einen Report an Domänen, die das wünschen



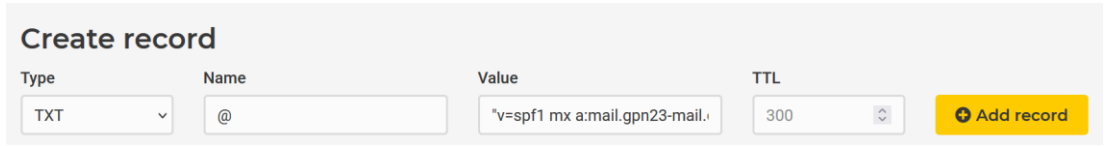
Einrichten von SPF und DKIM

Administration → E-Mail-Domains → Spalte: Aktionen → (Details)

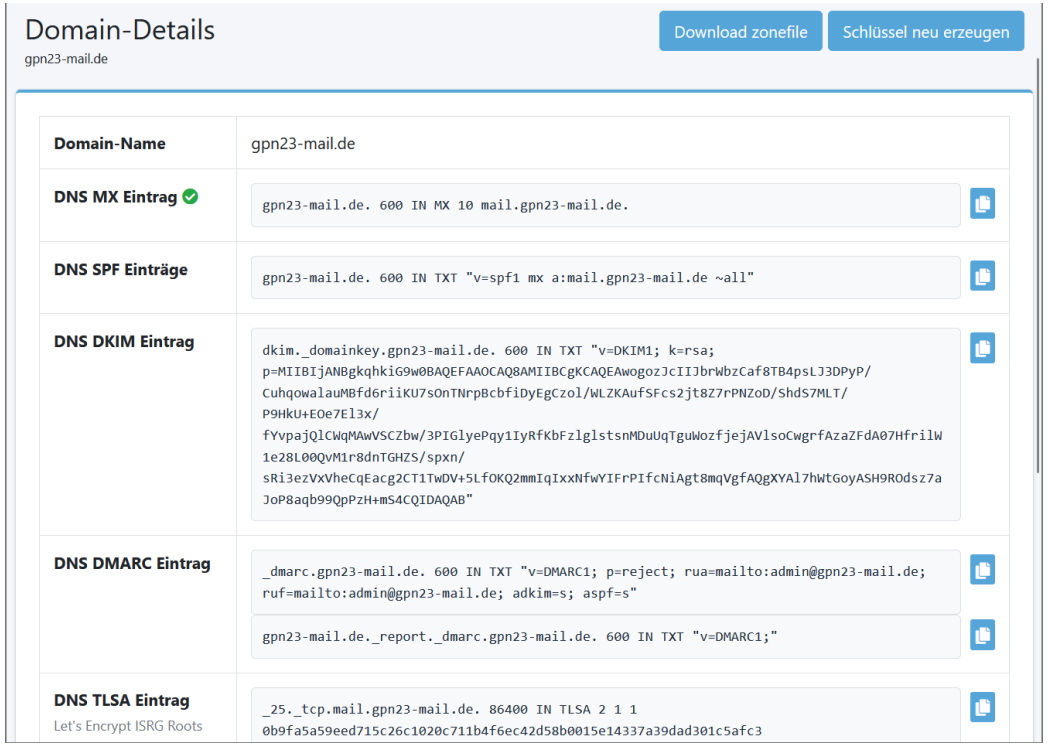
→ Schlüssel erzeugen

In Hetzner DNS Console

- SPF:



- DKIM (public key in DNS):



Einrichten von DMARC

_dmarc.gpn23-mail.de.

"v=DMARC1; p=reject; rua=mailto:admin@gpn23-mail.de; ruf=mailto:admin@gpn23-mail.de; adkim=s; aspf=s“

Zum Verifizieren:

SPF, DKIM, DMARC Setup testen → http://dmarctester.com

v → Version des Protokolls

p → policy (none, quarantine, reject)

rua (Reporting URI for Aggregate Data) → E-Mail-Adresse für (Tages-) Zusammenfassungen

ruf (Reporting URI for Forensic Data) → E-Mail-Adresse für Forensische Berichte (wird kaum noch versendet)

adkim → DKIM alignment mode (r=relaxed, s=strict)

aspf → SPF alignment mode (r=relaxed, s=strict)

Diese Einträge sollten jetzt im DNS vorhanden sein

Type	Name	Value	TTL	
A	mail .gpn23-mail.de	91.99.94.124	300	Delete record
MX	@	mail 10	300	Delete record
NS	@	helium.ns.hetzner.de.	3600	Delete record
NS	@	oxygen.ns.hetzner.com.	3600	Delete record
NS	@	hydrogen.ns.hetzner.com.	3600	Delete record
SOA	@	hydrogen.ns.hetzner.com. dns. ...	300	
TXT	_dmarc .gpn23-mail.de	"v=DMARC1; p=reject; rua=mailt...	300	Delete record
TXT	@	"v=spf1 mx a:mail.gpn23-mail.d ...	300	Delete record
TXT	dkim._domai gpn23-mail.de	"v=DKIM1; k=rsa; p=MIIBIjANBg ...	300	Delete record

Probleme mit @t-online.de

Delayed Mail (still being retried)

Von Mail Delivery System am 2025-06-09 07:26

Details Kopfzeilen

Delivery report (~563 B)

```
This is the mail system at host mail.gpn23-mail.de.

###################################################################
# THIS IS A WARNING ONLY.  YOU DO NOT NEED TO RESEND YOUR MESSAGE. #
###################################################################

Your message could not be delivered for more than 0 hour(s).
It will be retried until it is 5 day(s) old.

For further assistance, please send mail to postmaster.

If you do so, please include this problem report. You can
delete your own text from the attached returned message.

                   The mail system

<jens.dorfmueller@t-online.de>: host mx01.t-online.de[194.25.134.72] refused to
    talk to me: 554 IP=91.99.94.124 - Dialup/transient IP not allowed. Use a
    mailgateway or contact toda@rx.t-online.de if obsolete. (DIAL)

Reporting-MTA: dns; mail.gpn23-mail.de
```

T-Online betrachtet Hetzner IP-Adressen erst einmal als „dialup“

T-Online verlangt „Webseite mit unmittelbarer Kontaktmöglichkeit“ (siehe https://postmaster.t-online.de/#t4.1)

→ ich habe das mit einem Impressum gelöst

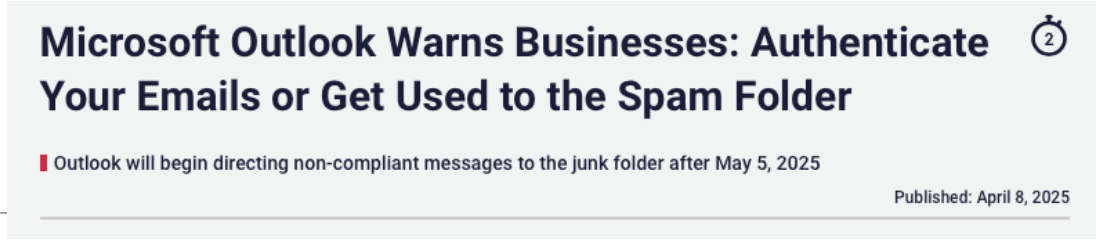
Danach:
freundliche E-Mail an toda@rx.t-online.de

→ wird dann manuell freigeschaltet!

tosa@rx.t-online.de fordert Impressum von Privatpersonen

Blis

Probleme mit Microsoft



Typischerweise outlook.com, hotmail.com, live.com

Outlook for Business ist tendenziell toleranter

Postmaster-Seite: https://sendersupport.olc.protection.outlook.com/pm/Postmaster

Outlook.com Smart Network Data Services: https://sendersupport.olc.protection.outlook.com/snds/index.aspx
The Outlook.com Smart Network Data Services (SNDS) gives you the data you need to understand and improve your reputation at Outlook.com.

domains sending more than 5,000 emails in a single day

SPF, DKIM und DMARC werden gefordert

“Non-compliant messages will first be routed to Junk,” Microsoft said, and eventually rejected if issues remain unresolved.

Tools von Gmail

E-Mails landen oft erst einmal im Spam-Ordner

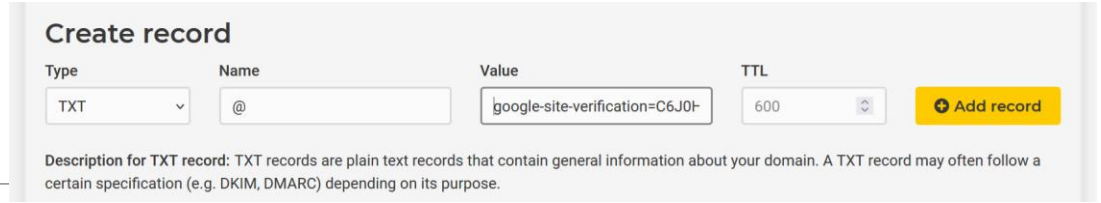
Google Postmaster Tools:
https://postmaster.google.com/

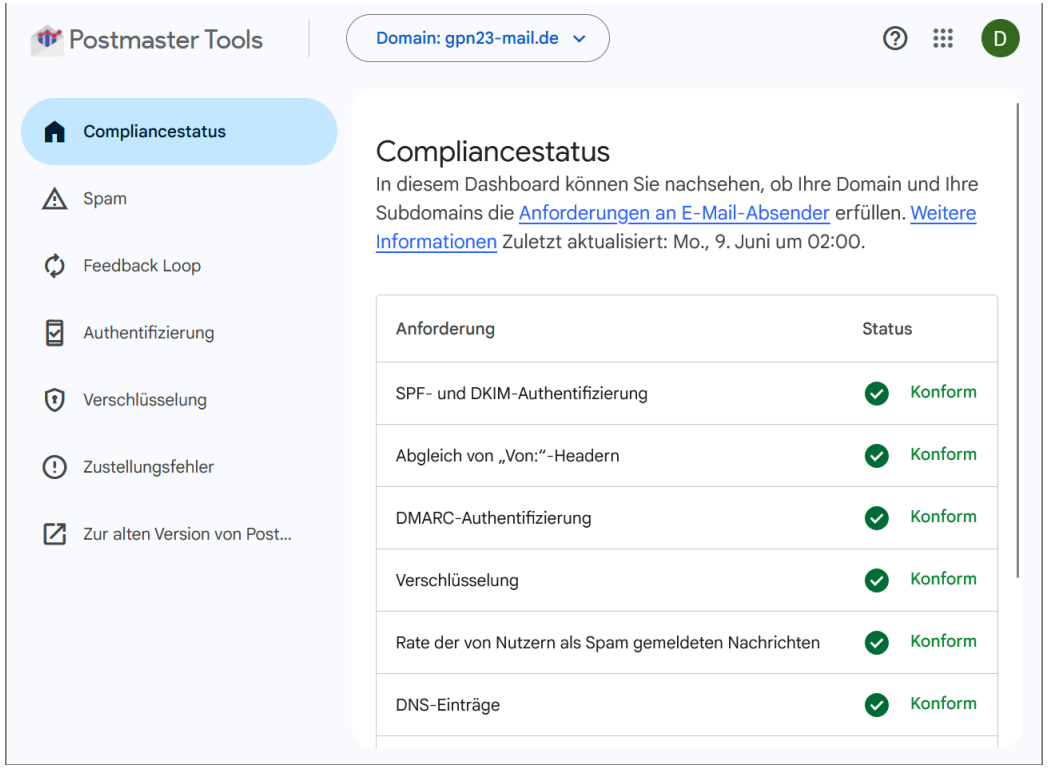
Domains können über TXT-record zu einer Liste von verifizierten Domains hinzugefügt werden

TXT-record mit „google-site-verification=<code>“ wird überprüft

Danach: im Dashboard Detail Infos
https://postmaster.google.com/v2/sender_compliance

Nach > 3 Jahren Server-Betrieb und exzellentem Rating auf Google Postmaster: Mails von neuen Adressen landen immer noch in Spam. ☹

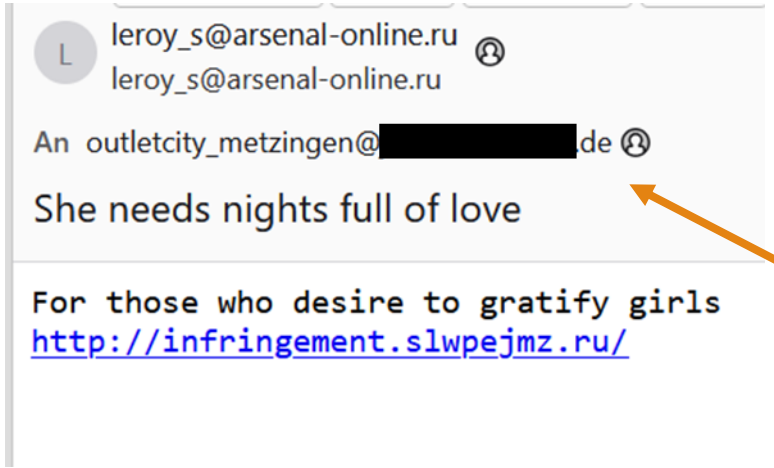




Ausblick: was kann man mit einem Mail-Server so machen

Weitere Domains anlegen

- Achtung: DNS-Einträge werden etwas komplizierter!
- Mit etwas Übung kann man innerhalb von 10 bis 15 Minuten ganz neue Domains online bekommen!



Catch-All Mail-Adressen

- Alias einrichten mit z.B. %@gpn23-mail.de
- … und „SQL LIKE Syntax nutzen“ anhaken
- Egal was vor dem @ steht, alles geht an einen E-Mail Account
- eine E-Mail pro Account; z.B.
  - amazon@gpn23-mail.de für Amazon
  - gpn23@gpn23-mail.de für die GPN23
  - hetzner@gpn23-mail.de für Hetzner
  - …
- Es wird sehr schön sichtbar, wenn ein Unternehmen Kontrolle über deine E-Mail-Adresse verloren hat!

Ausblick: DMARC Antworten auswerten

DMARC-Reports kommen als XML in zip-Datei

Tool zum Auswerten von DMARC Reports: https://hub.docker.com/r/gutmensch/dmarc-report

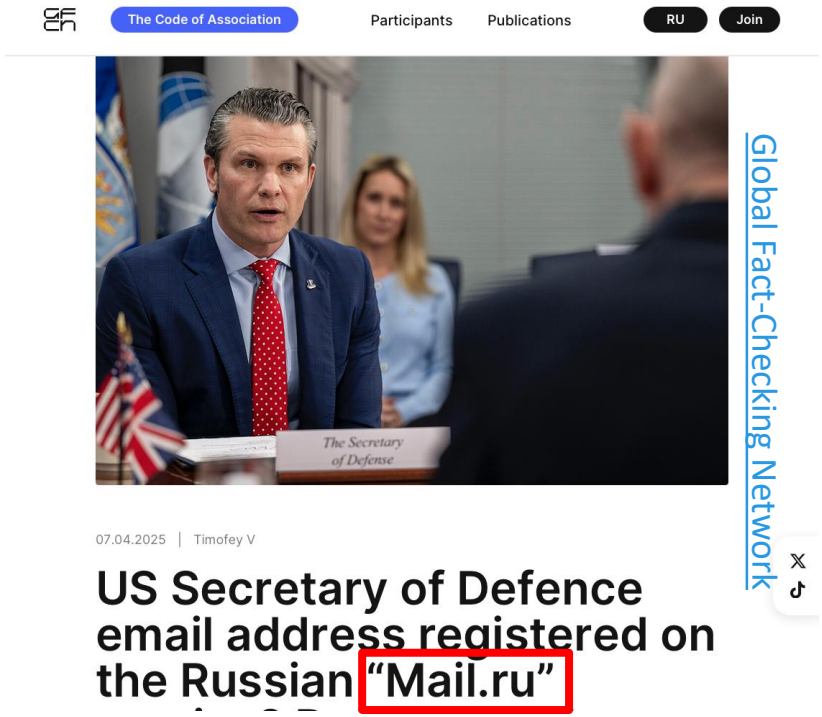
Basiert auf: https://github.com/techsneeze/dmarcts-report-viewer

DMARC Reports

Start Date	End Date ▼	Domain	Reporting Organization	Report ID	Messages
2025-02-12 0:00:00 UTC	2025-02-13 0:00:00 UTC	dorfmuller.de	Mail.Ru	89133326970021195341739318400	1
2025-02-12 0:00:00 UTC	2025-02-13 0:00:00 UTC	xn--dorfmller-u9a.de	Mail.Ru	48784779001502575551739318400	1
2025-02-11 0:00:00 UTC	2025-02-12 0:00:00 UTC	xn--dorfmller-u9a.de	Mail.Ru	19766787536526813017392320000	1

Report from Mail.Ru for dorfmuller.de
2025-02-12 0:00:00 UTC to 2025-02-13 0:00:00 UTC
Policies: adkim=s, aspf=s, p=reject, sp=reject, pct=100

IP ▲	Host Name	Message Count	Disposition	Reason	DKIM Domain	DKIM Auth	SPF Domain	SPF Auth	DKIM Align	SPF Align	DMARC
117.221.143.213	117.221.143.213	1	reject			unknown	dorfmuller.de	softfail	fail	fail	Fail
	Sum:	1									



Ausblick: DMARC Antworten auswerten

DMARC-Reports kommen als XML in zip-Datei

Tool zum Auswerten von DMARC Reports:
https://hub.docker.com/r/gutmensch/dmarc-report

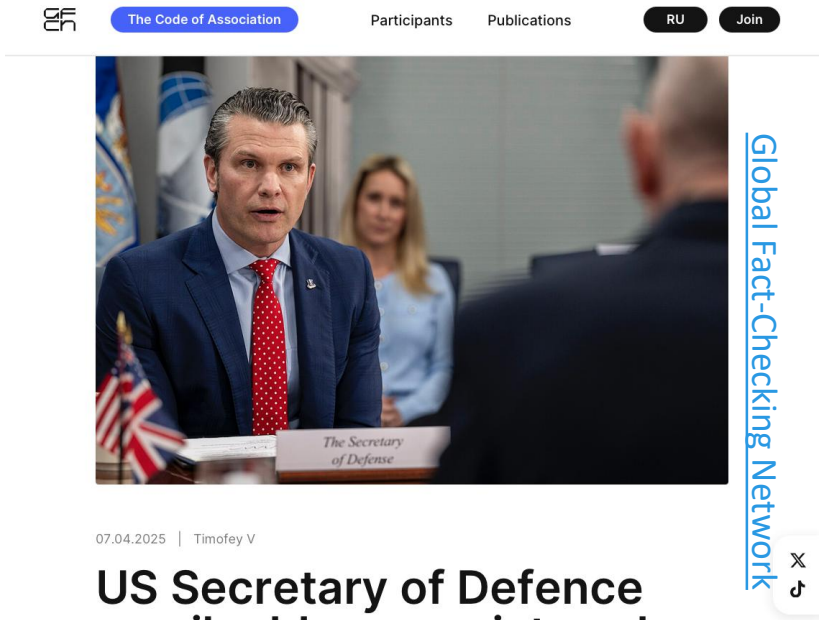
Basiert auf:
https://github.com/techsneeze/dmarcts-report-viewer

DMARC Reports

Start Date	End Date ▼	Domain	Reporting Organization	Report ID	Messages
2025-02-12 0:00:00 UTC	2025-02-13 0:00:00 UTC	dorfmuller.de	Mail.Ru	8913332697002119534173931840O	1
2025-02-12 0:00:00 UTC	2025-02-13 0:00:00 UTC	xn--dorfmller-u9a.de	Mail.Ru	4878477900150257555173931840O	1
2025-02-11 0:00:00 UTC	2025-02-12 0:00:00 UTC	xn--dorfmller-u9a.de	Mail.Ru	19766787536526813017392320O0	1

Report from Mail.Ru for dorfmuller.de
2025-02-12 0:00:00 UTC to 2025-02-13 0:00:00 UTC
Policies: adkim=s, aspf=s, p=reject, sp=reject, pct=100

IP ▲	Host Name	Message Count	Disposition	Reason	DKIM Domain	DKIM Auth	SPF Domain	SPF Auth	DKIM Align	SPF Align	DMARC
117.221.143.213	117.221.143.213	1	reject			unknown	dorfmuller.de	softfail	fail	fail	Fail
	Sum:	1									



Global Fact-Checking Network

Vielen Dank …

… für eure Aufmerksamkeit!

Zusatzinfo: Einrichten von DMARC (für weitere Domains)

EMPFÄNGER IN SELBER DOMAIN (ODER EINE SUB-DOMAIN) DER RUA- UND RUF-DOMAIN

Name:
_dmarc.gpn23-mail.de.

Value:
"v=DMARC1; p=reject; rua=mailto:admin@gpn23-mail.de; ruf=mailto:admin@gpn23-mail.de; adkim=s; aspf=s“

EMPFÄNGER IN ANDERER DOMAIN

Name:
_dmarc.<other-domain>.

Value:
"v=DMARC1; p=reject; rua=mailto:admin@<ruf-/rua-domain>; ruf=mailto:admin@<ruf-/rua-domain>; adkim=s; aspf=s“

Name:
gpn23-mail.de._report._dmarc.<ruf-/rua-domain>

Value:
"v=DMARC1;"

Mit diesem zweiten Eintrag bestätigt der Besitzer von <ruf-/rua-domain>, dass er die DMARC-Mails empfangen möchte.

Zusatzinfo: Impressum hinzufügen

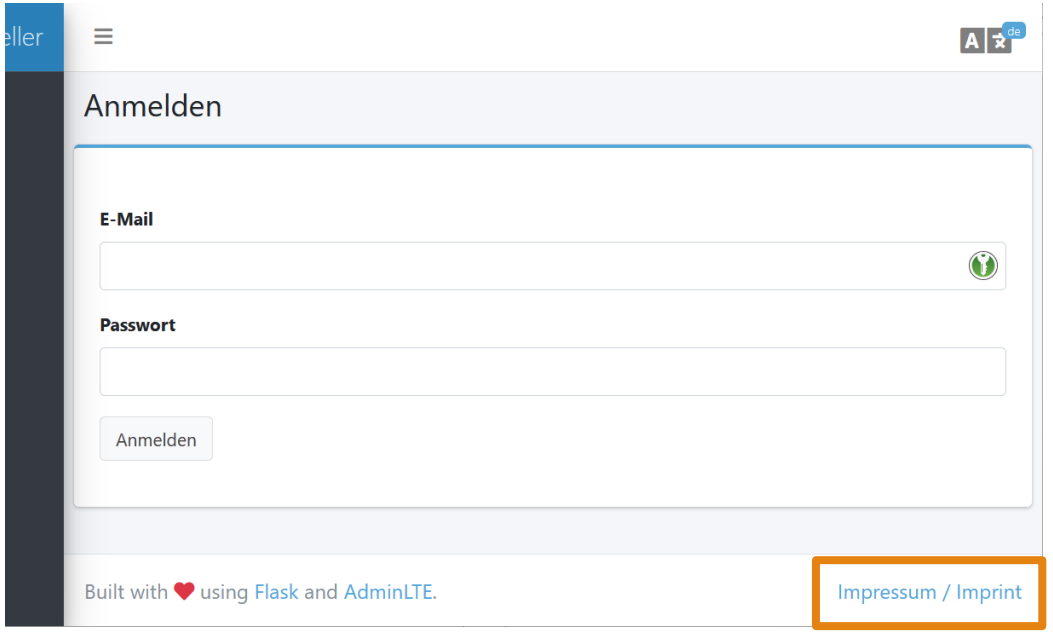
```
cd /mailu

wget https://github.com/Mailu/Mailu⏎
/raw/refs/heads/master/core/admin/ ⏎
mailu/sso/templates/base_sso.html
```

In Template: Link auf Github durch Impressum ersetzen (siehe diff unten)

Im container „admin“ unter „volumes“ folgende Zeile hinzufügen:

```
- "./base_sso.html:/app/mailu/sso ⏎
/templates/base_sso.html"
```




```
root@gpn23-mail.de:~# diff base_sso.html /opt/mailu/mailu/base_sso.html
<    <i class="fa fa-code-branch" aria-hidden="true"></i><span class="sr-only">fork</span>
<    on <a href="https://github.com/Mailu/Mailu">Github</a>
---
>    <a href="https://www.gpn23-mail.de/imprint.html">Impressum / Imprint</a>
```