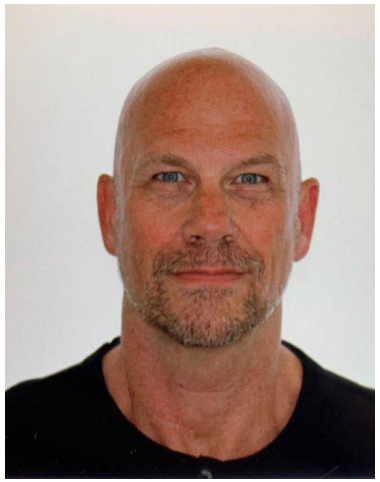
Tax Administration

How to Detect that Your Domains are Being Abused for Phishing by Using DNS

Karl Lovink – Dutch Tax and Customs Administration

Arnold Hölzel - SMT Simple Management Technologies

About us



Karl Lovink
Technical Lead SOC
Dutch Tax and Customs Administration
kw.lovink@belastingdienst.nl

Arnold Hölzel
Senior Security Consultant
Simple Management Technologies
arnold.holzel@smtware.com

Bring it to the core

Why do we combat phishing attacks?

- Why is fighting phishing so important?
  - Damage for citizens and businesses;
  - Losing trust in the relationship between the Taxpayer and the Dutch Tax and Customs Administration.

- Important to discover phishing campaigns as soon as possible.

- Break the money circle, it’s all about money.

A phishing example

Van: Belastingdienst <belastingaangifte@belastingdienst.nl>

Datum:23-08-2015 11:05:10 CEST

Aan: xxxxxx@planet.nl

Onderwerp: Belastingaangifte 2014

Bij controle van onze administratie hebben wij geconstateerd dat er een betalingsachterstand is ontstaan van uw belastingaangifte 2014. Wij hebben geprobeerd om het openstaande bedrag te incasseren, helaas is dit niet gelukt op het rekeningnummer dat bij ons bekend staat. Het huidige openstaande bedrag bedraagt 83,04 euro. U ontvangt ook een schriftelijke herinnering die vandaag per post is verstuurd. Thans verzoeken wij u vriendelijk om dringend het openstaand bedrag van ...

Te betalen u kunt het bedrag overmaken naar bankrekeningnummer NL62ABNA XXXXXXXXX tnv belastingdienst" onder vermelding van betalingskenmerk BTW038372293N Als u deze betaling heeft voldaan kunt u de brief als niet verzonden beschouwen. Als u binnen acht dagen deze rekening niet heeft voldaan dan verzenden wij geen aanmaning en hierbij worden incasso kosten gerekend Ik hoop u voldoende geinformeerd te hebben. Wij zien uw betaling graag tegemoet en danken u voor uw medewerking.

Met vriendelijke groet,

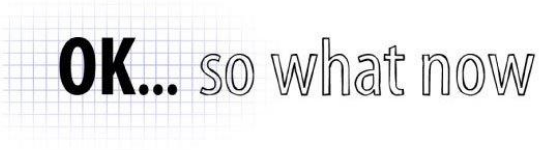
Robert Versteegen

Directeur Belastingdienst

N.B. Dit is een automatisch verzonden e-mail, het is niet mogelijk deze e-mail te beantwoorden.

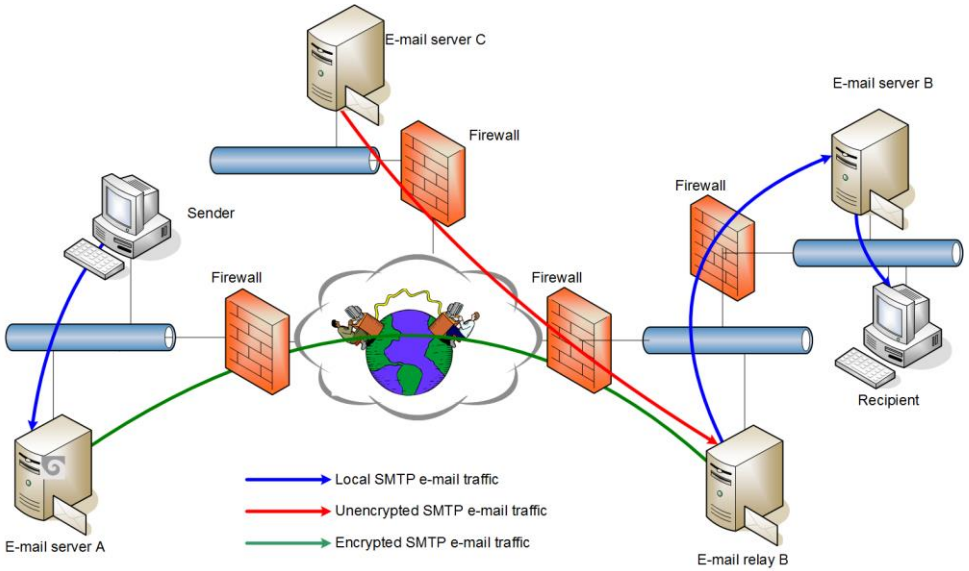
OK… so what now!

- Starting points:
  - Change may not impact the business.
  - Using standards:
    - STARTTLS;
    - DNS-based Authentication of Named Entities;
    - SMTP MTA Strict Transport Security;
    - Sender Policy Framework;
    - DomainKeys Identified Mail;
    - Domain-based Message Authentication, Reporting and Conformance.



STARTTLS

- STARTTLS is used to upgrade an un-secure plaint text connection to a secure encrypted connection.
- Used between e-mail servers to communicate over un-secure networks.
- More info:
  - RFC3207 - SMTP Service Extension for Secure SMTP over Transport Layer Security.



DNS-Based Authentication of Named Entities

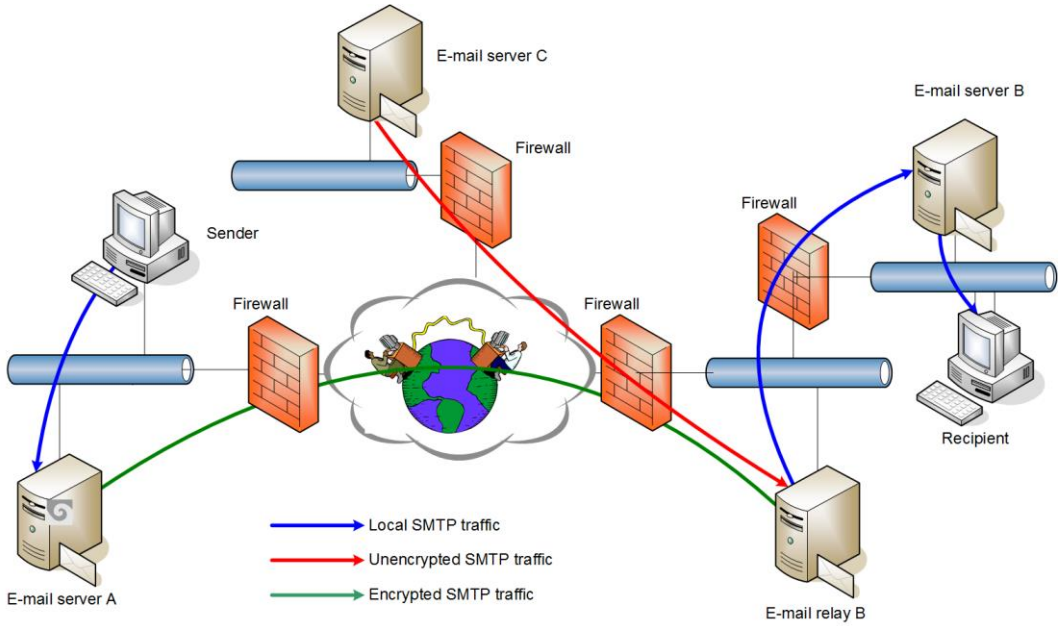
- DANE = DNS-Based Authentication of Named Entities.
- DANE allows to advertise TLS support through a TLSA TXT resource record.
- More info:
  - RFC6698 - DNS-Based Authentication of Named Entities;
  - RFC7672 - DANE for SMTP.

ars TECHNICA

BIZ & IT —

Don’t count on STARTTLS to automatically encrypt your sensitive e-mails

TLS stripping and DNS attacks allow eavesdropping on protected messages.



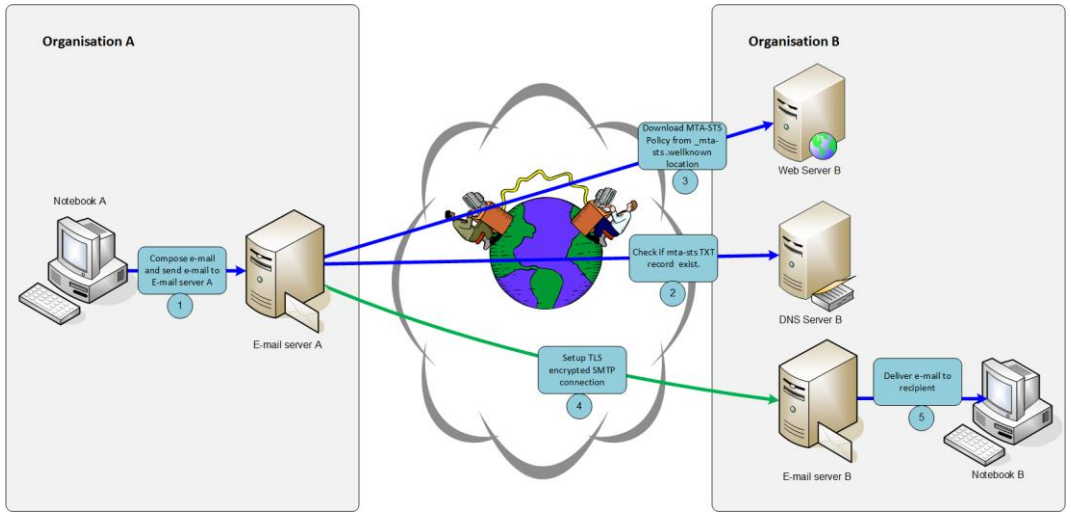
DNS-Based Authentication of Named Entities

- Example: belastingdienst.nl
- TLSA TXT resource record:

```
_25._tcp.smtp1.belastingdienst.nl. IN TLSA 3 1 1 \
 b169456b9f12cecc88bfdc9e82dc4f2546a779e6cad0be9751d12e51654e898a
_25._tcp.smtp2.belastingdienst.nl. IN TLSA 3 1 1 \
 b3c1e98bf0c76de6af8905755fcd073400d99503de9c699b4b8f232b9b36b02b
```

SMTP Mail Transfer Agent Strict Transport Security

- MTA-STS = Mail Transfer Agent Strict Transport Security.
- MTA-STS allows a receiving e-mail domain to publish their TLS policy.
- More info:
  - RFC8461 - SMTP Mail Transfer Agent Strict Transport Security;
  - RFC8460 - SMTP TLS Reporting.
- RFC published September 2018.
- Implementation:
  - gmail.com April 2019;
  - belastingdienst.nl **June 2019**.



SMTP Mail Transfer Agent Strict Transport Security

- Example: belastingdienst.nl
- MTA-STS/TLS-RPT resource records:

```
mta-sts.belastingdienst.nl.   IN A   85.159.98.22
_mta-sts.belastingdienst.nl.      IN TXT "v=STSv1;\
    id=20190624163600"
_smtp._tls.belastingdienst.nl.    IN TXT "v=TLSRPTv1;\
    rua=mailto:mta-sts@belastingdienst.nl"
```

SMTP Mail Transfer Agent Strict Transport Security

- Example: belastingdienst.nl
- URL: https://mta-sts.belastingdienst.nl/.well-known/mta-sts.txt
  - MTA-STS Policy file:

```
version: STSv1
mode: testing
mx: smtp1.belastingdienst.nl
mx: <additional MX records>
max_age: 86400
```

SMTP MTA-STS Reporting – The GOOD

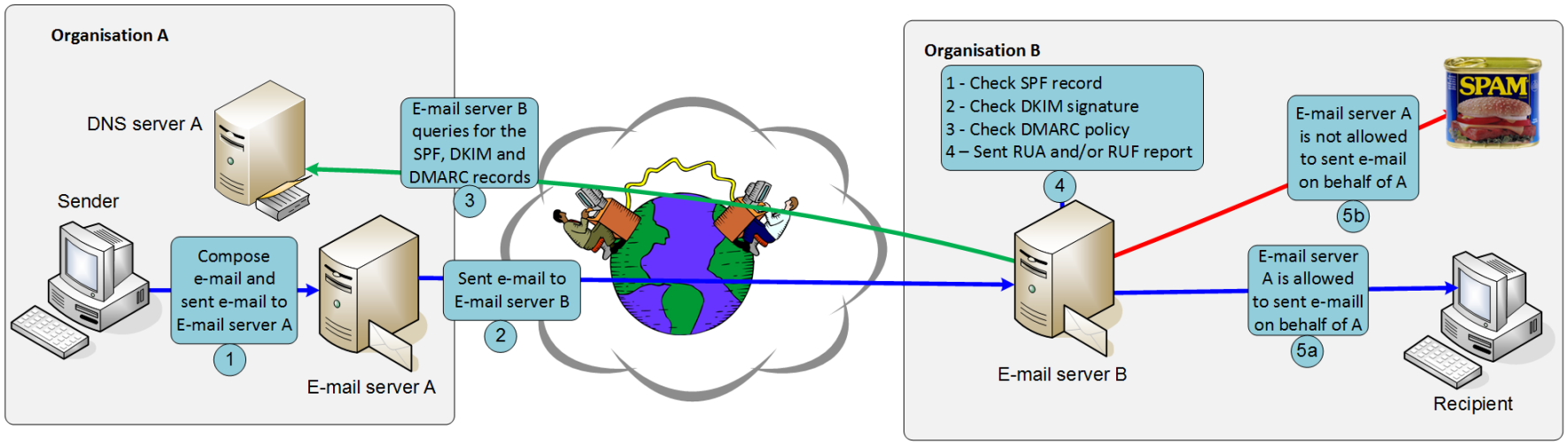

```
{"organization-name":"Google Inc.",
      "date-range":{
            "start-datetime":"2019-06-24T00:00:00Z",
            "end-datetime":"2019-06-24T23:59:59Z"},
      "contact-info":smtp-tls-reporting@google.com,
      "report-id":"2019-06-25T00:00:00Z_belastingdienst.nl",
      "policies":[
            {"policy":
                  {"policy-type":"sts",
                        "policy-string":[
                        "version: STSv1",
                        "mode: testing",
                        "mx: <MX records>",
                        "max_age: 10368000"],
                  "policy-domain":"belastingdienst.nl",
                "summary":{
                      "total-successful-session-count":1} } ]
}
```

SMTP MTA-STS Reporting – The BAD

```
{"organization-name":"Google Inc.",
      . . . . . .
      "summary": { "total-failure-session-count": 1 },
      "failure-details": [
            {
            "result-type": "starttls-not-supported",
            "sending-mta-ip": "192.51.100.45",
            "receiving-ip": "203.0.113.90",
            "receiving-mx-hostname": "smtp.example.com",
            "failed-session-count": 1
            }
      ]
      . . . . . .
}
```

Sender Policy Framework

- SPF = Sender Policy Framework.
- Validates if an e-mail is sent from a valid IP address or domain.
- Check is done against SPF TXT resource records in the DNS.
- More info: RFC7208 - Sender Policy Framework (SPF), Version 1.



How can we detect phishers when they not using our infrastructure?

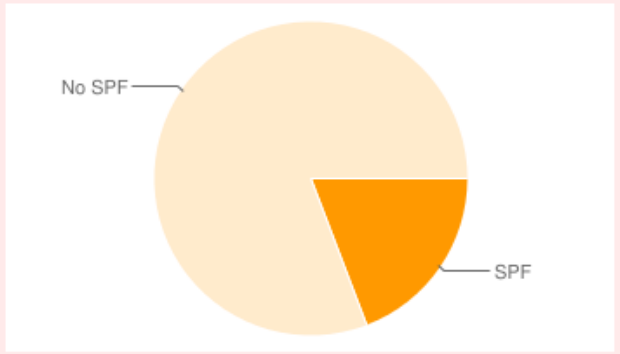
If everything happens on the Internet and not on our servers?

Sender Policy Framework

- Paragraph 7.2 – Macro Definitions.
- You need access to your DNS query and response log.
- 0.049% of registered domains have macros in their SPF TXT records*.

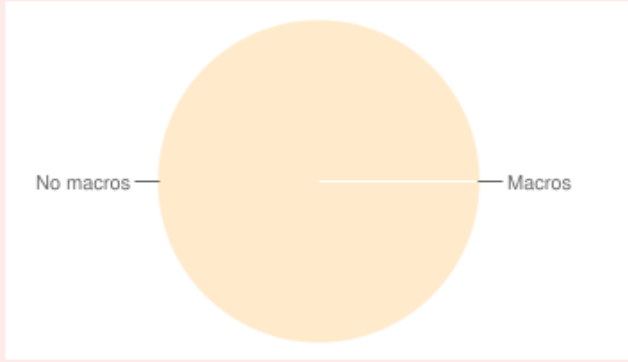
All Domains

Total Domains	140137379	100.0%
Domains with SPF	26910393	19.2%
Domains without SPF	113226986	80.8%



Domains With SPF Record Macros

Domains with SPF	26910393	100.000%
Macros	13172	0.049%
No macros	26897221	99.951%



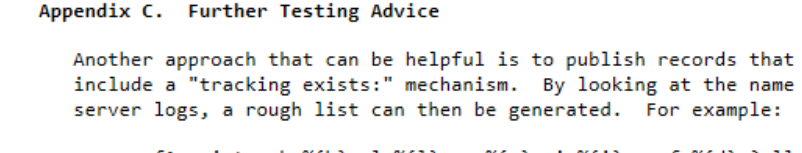
- Gives you an e-mail track-and-trace system.

*Source: https://spf-all.com/stats.html

Sender Policy Framework

- By using macros in the SPF TXT resource records you get visibility on:
  - %s - Complete sender e-mail address;
  - %h - HELO/EHLO of the sending e-mail server;
  - %l - Local-part of the sending e-mail address;
  - %o - Domain-part of the sending e-mail address;
  - %i - IP address of the sending e-mail server.

- **Be aware** %l and %s will introduce a privacy-issue! There will be valid e-mail addresses in resolver logs!



Appendix C. Further Testing Advice

Another approach that can be helpful is to publish records that include a "tracking exists:" mechanism. By looking at the name server logs, a rough list can then be generated. For example:

Sender Policy Framework

- Example: belastingdienst.nl
- Basic SPF implementation.
- SPF TXT resource record:

```
belastingdienst.nl IN TXT v=spf1 mx a:mailer1.belastingdienst.nl \
   a:mailer2.belastingdienst.nl a:smtp11.belastingdienst.nl \
   a:smtp12.belastingdienst.nl -all
```

- Do not forget your subdomains! (and there subdomains, and there….)

```
*.belastingdienst.nl IN TXT "v=spf1 -all"
*.acc.belastingdienst.nl IN TXT "v=spf1 -all"
```

Sender Policy Framework

- Example: belastingdienst.nl
- Advanced SPF implementation with macros.
- The SPF redirect resource record:

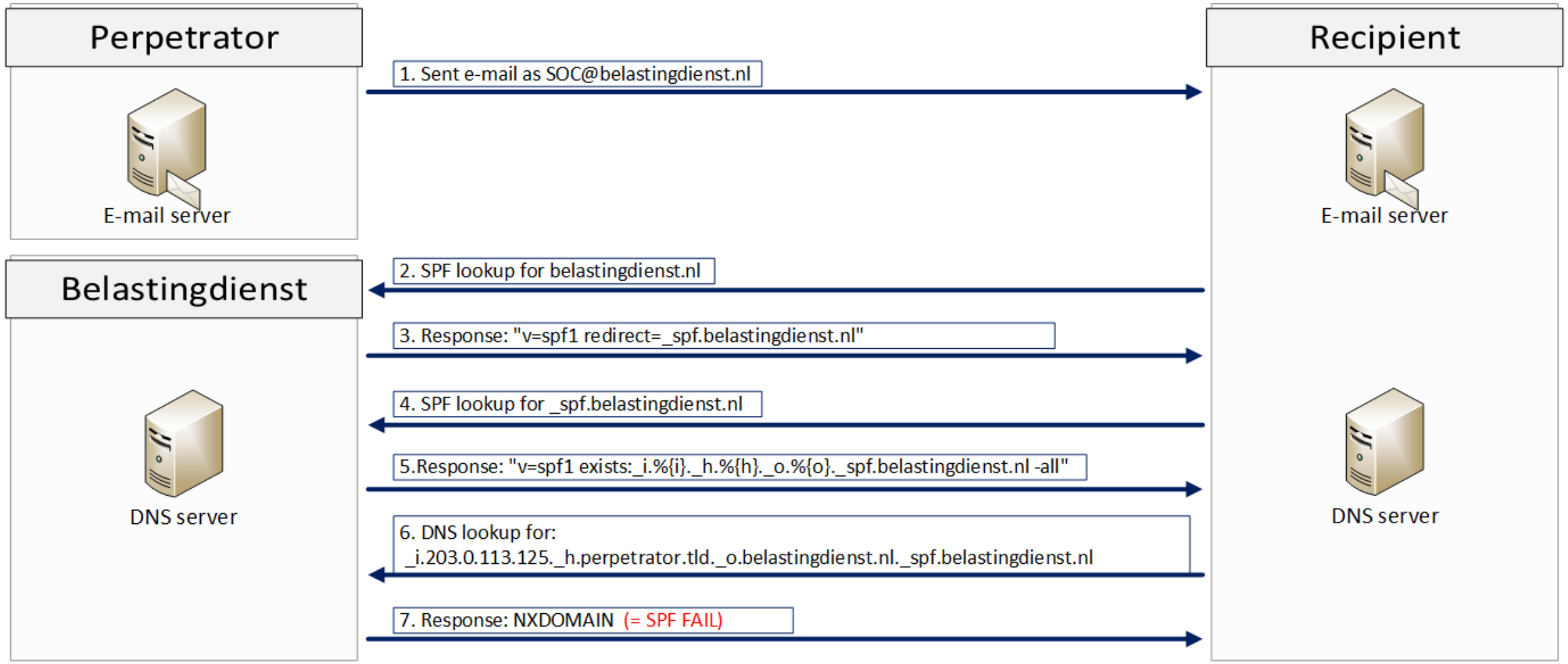
```
belastingdienst.nl. IN TXT "v=spf1 redirect=_spf.belastingdienst.nl"
```

- The SPF exists resource record and macros:

```
_spf.belastingdienst.nl IN TXT "v=spf1 \
   exists:_i.%{i}._h.%{h}._o.%{o}._spf.belastingdienst.nl -all"
_i.85.159.101.15._h.smtp2.belastingdienst.nl._o.belastingdienst.nl.\
  _spf.belastingdienst.nl. IN A 127.0.0.1
_i.85.159.101.15._h.belastingdienst.nl._o.belastingdienst.nl.\
  _spf.belastingdienst.nl. IN A 127.0.0.1
```

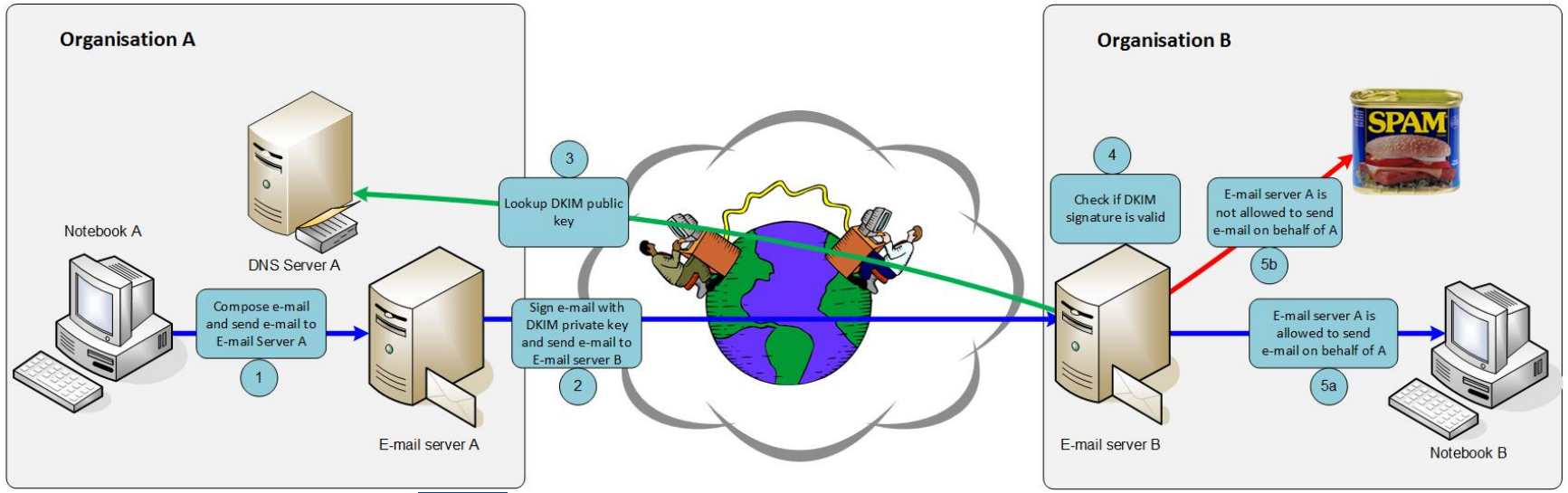
Sender Policy Framework – The Good

Sender Policy Framework – The Bad



DomainKeys Identified Mail

- DKIM = DomainKeys Identified Mail.
- Signs body and selected parts of the SMTP header.
- Signature is transmitted in a DKIM-signature header.
- Public DKIM key is stored in the DNS as a TXT resource record.
- More info: RFC6376 - DomainKeys Identified Mail (DKIM) Signatures.



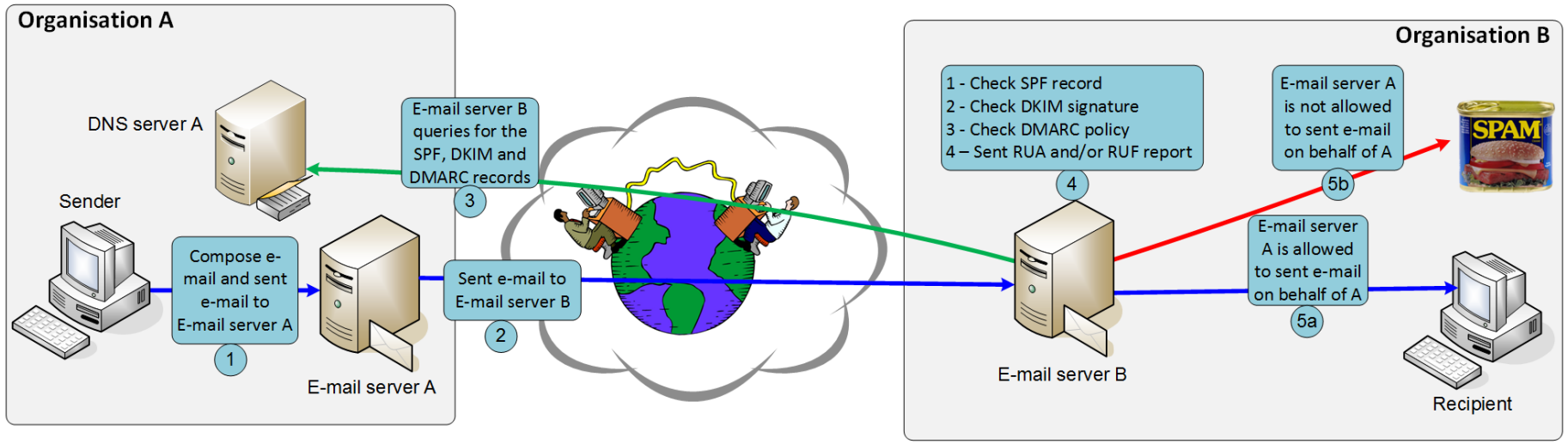
DomainKeys Identified Mail

- Example: belastingdienst.nl:201707
- A DKIM selector is needed. Can be found in the header of the e-mail.
- DKIM TXT resource record:

```
201707._domainkey.belastingdienst.nl IN TXT "v=DKIM1;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyzXWCOzeB5qsw
ey69WrHNeqdgnNUiFJkT/EMjm78h1zMXkrd6t0VtTB4rAe39/BlwNFC0jKs
kE3u1nl6whfQX3fT/68xr2SdcOp6j/DTtS6rC1EWFXyawX6NfxM/Pt8DV5C
LDFGHMht63LetGyiQYv+TrBBiATPjfLPgrArx7jaAoPv0Az/ec86rl+Q9jX
A0QO7zR6Ih""0TIJYwnzVf/7Dsl4GpsmZsN1oEaXhauuDuynQsHm9iptzKC
8IKHaGr9g8qPnh8PDAm0QJSWAq5j1h12j7qjMLwOMEwPKwCE9HnWzeUpzxa
JDHL2K4dHYkXF6ErRjLhtTU2Mx6/F+7Ku4wQIDAQAB;"
```

Domain-based Authentication, Reporting & Conformance

- DMARC = Domain-based Authentication, Reporting &. Conformance.
- How to deal with the results of the SPF and / or DKIM checks of received e-mails.
- More info: RFC7489 - Domain-based Message Authentication, Reporting, and Conformance



Domain-based Authentication, Reporting & Conformance

- Example: belastingdienst.nl
- DMARC TXT resource record:

```
_dmarc.belastingdienst.nl IN TXT "v=DMARC1; p=reject;
      rua=mailto:dmarc.rua@belastingdienst.nl; sp=reject;"
```

- **Be aware** The ruf-tag defines the e-mail address where forensics reports must be sent to. Be aware of privacy issues! RUF reports contain parts of the original e-mail body.

Summarization of the standards

- Implementation of these standards give you more detection and prevention capabilities.
- Implementation of these standards can be done. We have ~550 domains. It took us about 1 month to implement.
- For prevention: both sender as recipient must implement these standards.
- Dutch Governmental Organizations must comply to Dutch Standardization Platform comply or explain list.
- SIDN announced a financial incentive DMARC and STARTTLS.

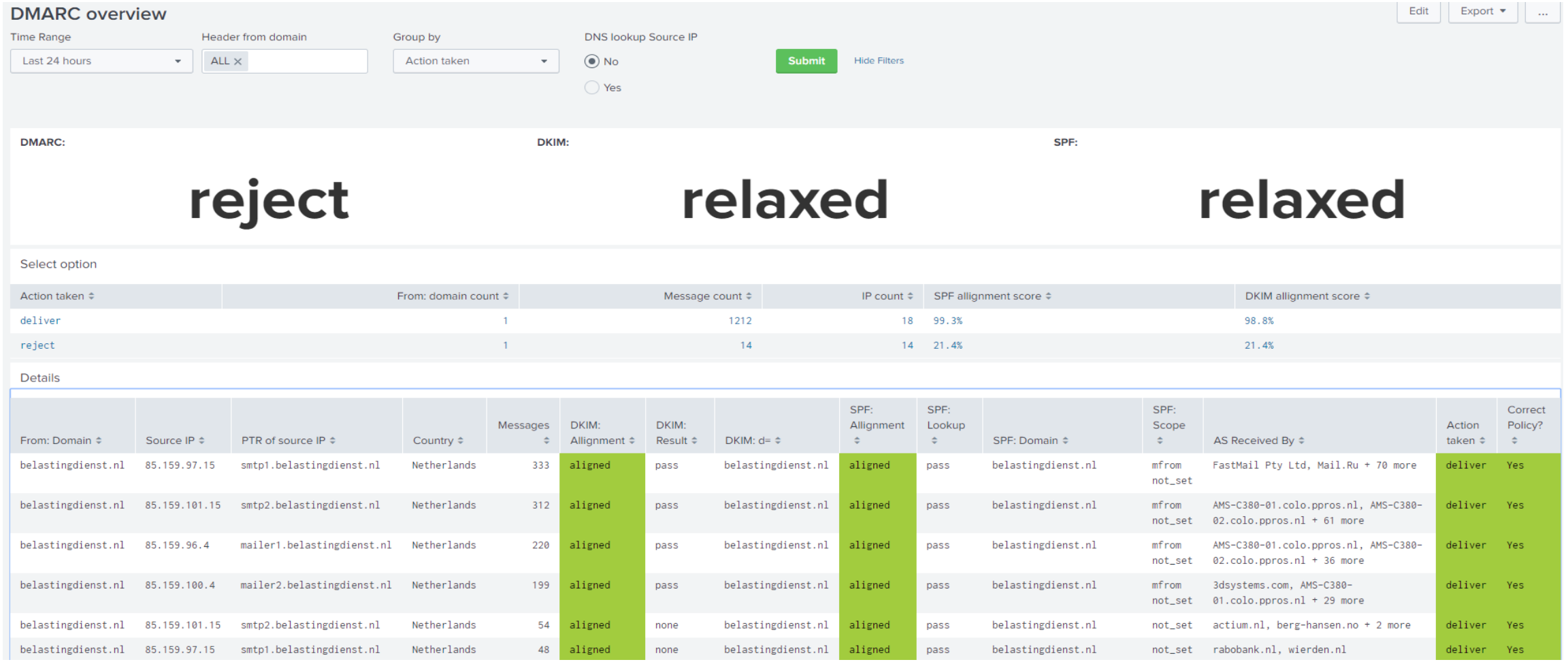
Now what, with all that info?

- Great info > do something with it:
  - DMARC > more insight in to what is happening on the receiving side;
  - SPF record > where are the e-mails coming from.

DMARC RUA Reports

- Delivered through e-mail as *.XML or *.XML.GZ
- The RUA e-mails are processed by Python scripts to use for dashboarding.
  - Output in key=value pair OR in JSON.
- You need to have:
  - a DMARC record in your DNS zone file;
  - network access to the RUA e-mail box by either using POP3(s) or IMAP(s);
  - The user-id and the password for the RUA mailbox.

DMARC Dashboards



DMARC overview

Edit | Export | ...

Time Range: Last 24 hours | Header from domain: ALL | Group by: Action taken | DNS lookup Source IP: No / Yes | Submit | Hide Filters

DMARC:	DKIM:	SPF:
reject	relaxed	relaxed

Select option

Action taken	From: domain count	Message count	IP count	SPF allignment score	DKIM allignment score
deliver	1	1212	18	99.3%	98.8%
reject	1	14	14	21.4%	21.4%

Details

From: Domain	Source IP	PTR of source IP	Country	Messages	DKIM: Allignment	DKIM: Result	DKIM: d=	SPF: Allignment	SPF: Lookup	SPF: Domain	SPF: Scope	AS Received By	Action taken	Correct Policy?
belastingdienst.nl	85.159.97.15	smtp1.belastingdienst.nl	Netherlands	333	aligned	pass	belastingdienst.nl	aligned	pass	belastingdienst.nl	mfrom not_set	FastMail Pty Ltd, Mail.Ru + 70 more	deliver	Yes
belastingdienst.nl	85.159.101.15	smtp2.belastingdienst.nl	Netherlands	312	aligned	pass	belastingdienst.nl	aligned	pass	belastingdienst.nl	mfrom not_set	AMS-C380-01.colo.ppros.nl, AMS-C380-02.colo.ppros.nl + 61 more	deliver	Yes
belastingdienst.nl	85.159.96.4	mailer1.belastingdienst.nl	Netherlands	220	aligned	pass	belastingdienst.nl	aligned	pass	belastingdienst.nl	mfrom not_set	AMS-C380-01.colo.ppros.nl, AMS-C380-02.colo.ppros.nl + 36 more	deliver	Yes
belastingdienst.nl	85.159.100.4	mailer2.belastingdienst.nl	Netherlands	199	aligned	pass	belastingdienst.nl	aligned	pass	belastingdienst.nl	mfrom not_set	3dsystems.com, AMS-C380-01.colo.ppros.nl + 29 more	deliver	Yes
belastingdienst.nl	85.159.101.15	smtp2.belastingdienst.nl	Netherlands	54	aligned	none	belastingdienst.nl	aligned	pass	belastingdienst.nl	not_set	actium.nl, berg-hansen.no + 2 more	deliver	Yes
belastingdienst.nl	85.159.97.15	smtp1.belastingdienst.nl	Netherlands	48	aligned	none	belastingdienst.nl	aligned	pass	belastingdienst.nl	not_set	rabobank.nl, wierden.nl	deliver	Yes

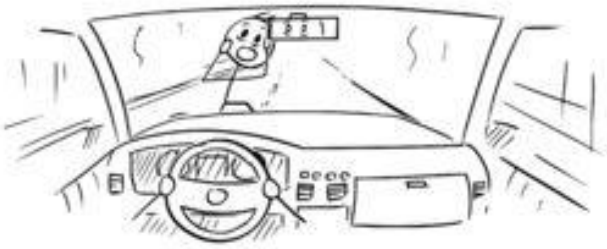
DMARC Dashboards

GREEN: Authorized e-mail servers, RED: Possible malicious e-mail servers

SPF Dashboarding

- Get even more insight in where e-mail is coming from and going to.
- You need:
  - to have a SPF record with macros:

    `_i.%{i}._h.%{h}._o.%{o}._spf.belastingdienst.nl`
  - to have your DNS query logging enabled;
  - to ingest your DNS log in log management system;
  - to know the good DNS queries.



SPF Dashboarding (The Good)

Sending server IP	HELO/EHLO	Country	FROM email domain	SPF server?	DNS response	Querying IP	DNS Hits	note
85.159.96.4	mailer1.belastingdienst.nl	Netherlands	belastingdienst.nl	Yes	NOERROR	104. .28 104. .253 104. .225 104. .133 104. .134 + 2084 more	7510	-
85.159.100.4	mailer2.belastingdienst.nl	Netherlands	belastingdienst.nl	Yes	NOERROR	103. .250 103. .161 104. .28 104. .253 104. .225 + 2040 more	7367	-
85.159.101.15	smtp2.belastingdienst.nl	Netherlands	belastingdienst.nl	Yes	NOERROR	104. .28 104. .253 104. .225 104. .133 104. .134 + 1331 more	4588	-

SPF Dashboarding (The Badly Configured)

Sending server IP	HELO/EHLO	Country	FROM email domain	SPF server?	DNS response	Querying IP	DNS Hits	note
85.159.100.4	unknown	Netherlands	belastingdienst.nl	Yes	NXDOMAIN	104. .132 149. .249 172. .11 172. .15 172. .9 + 36 more	553	-
85.159.96.4	localhost	Netherlands	belastingdienst.nl	Yes	NXDOMAIN	173. .111 173. .75 173. .77 194. .49 208. .21 + 16 more	94	-
85.159.97.15	localhost	Netherlands	belastingdienst.nl	Yes	NXDOMAIN	172. .10 172. .3 173. .100 173. .75 173. .77 + 21 more	83	-

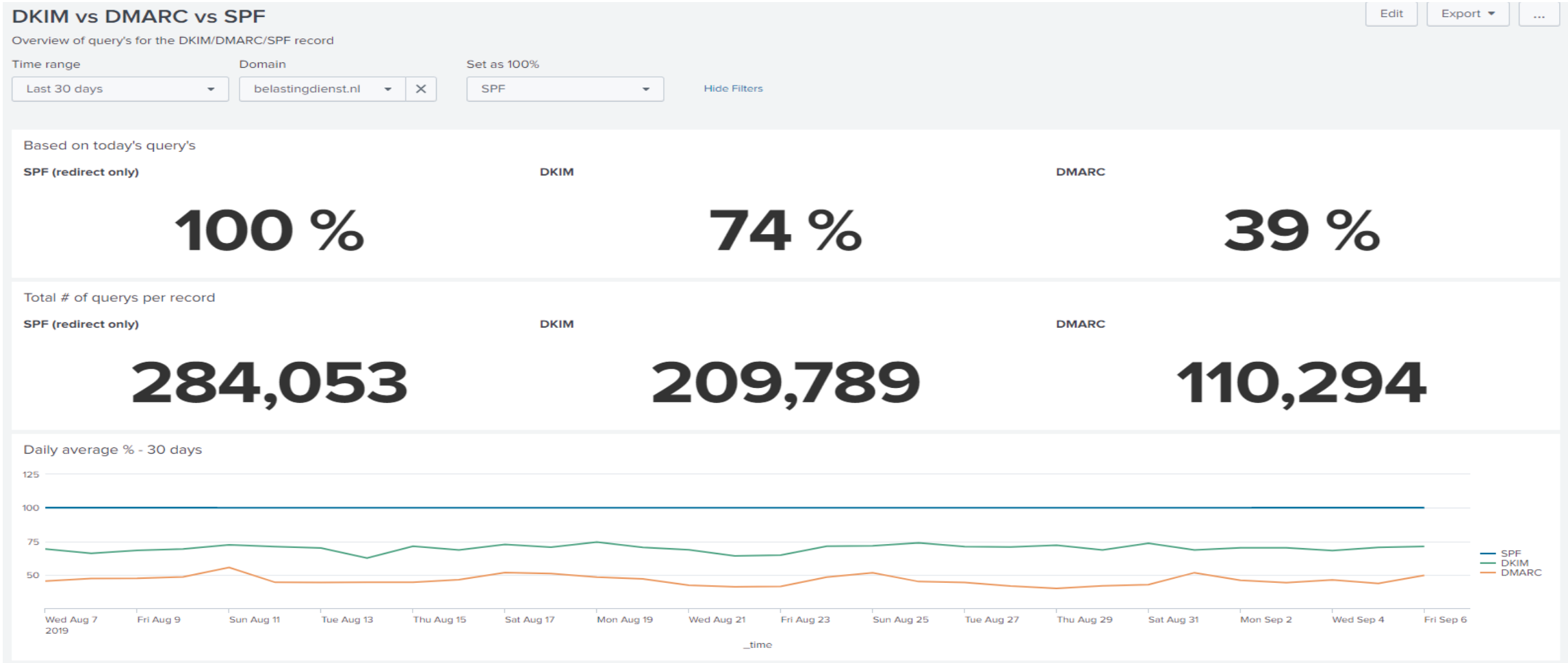
SPF Dashboarding (The Evil!)

Sending server IP	HELO/EHLO	Country	FROM email domain	SPF server?	DNS response	Querying IP	DNS Hits	Note
190. .202	forward24o.mail.yandex.net	Colombia	vrnacnpoenyr.loopbaanlab.info	No	NXDOMAIN	185. .30 94. .126	14	-
123. .147	forward508o.mail.yandex.net	Sri Lanka	kutgsboh.loopbaanlab.info	No	NXDOMAIN	217. .245 94. .123 94. .124	6	-
96. .253	forward2o.mail.yandex.net	United States	afpdxywdl.loopbaanlab.info	No	NXDOMAIN	185. .30 94. .126	6	-
183. .62	forward767o.mail.yandex.net	Thailand	syxcmwfx.loopbaanlab.info	No	NXDOMAIN	185. .30 94. .126	3	-
197. .128	forward4o.mail.yandex.net	Zambia	sdlmgczzvo.loopbaanlab.info	No	NXDOMAIN	185. .30 94. .126	3	-
37. .246	forward40o.mail.yandex.net	Azerbaijan	ucevuqqppng.loopbaanlab.info	No	NXDOMAIN	185. .30 94. .126	3	-
141. .222	forward7o.mail.yandex.net	Armenia	oayqvh.loopbaanlab.info	No	NXDOMAIN	94. .123	2	-

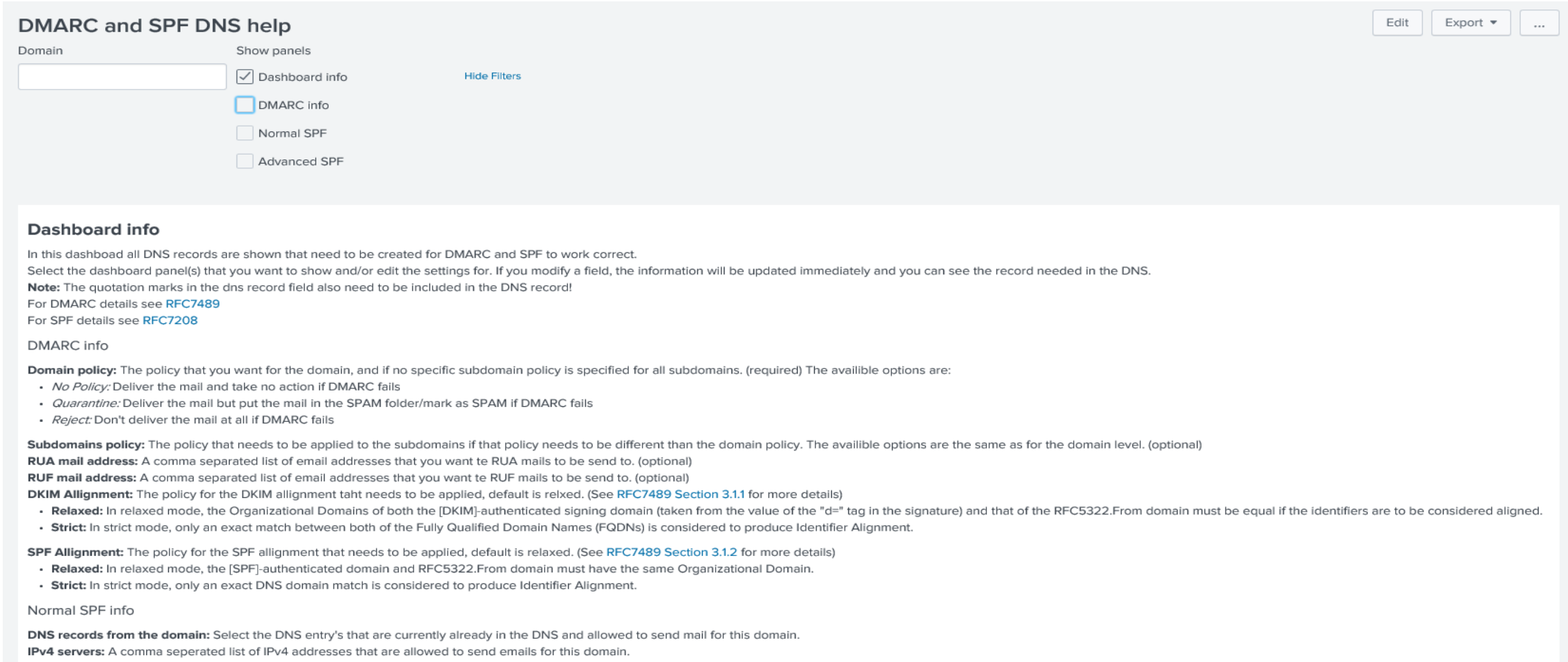
There is more?

- Python script to resolve your SPF record and fill the lookup table.
- More dashboards:
  - RFC7208, SPF info;
  - RFC7489, DMARC info;
  - Number of query’s per record type;
  - DNS record help for:
    - DMARC records;
    - (Advanced) SPF record.

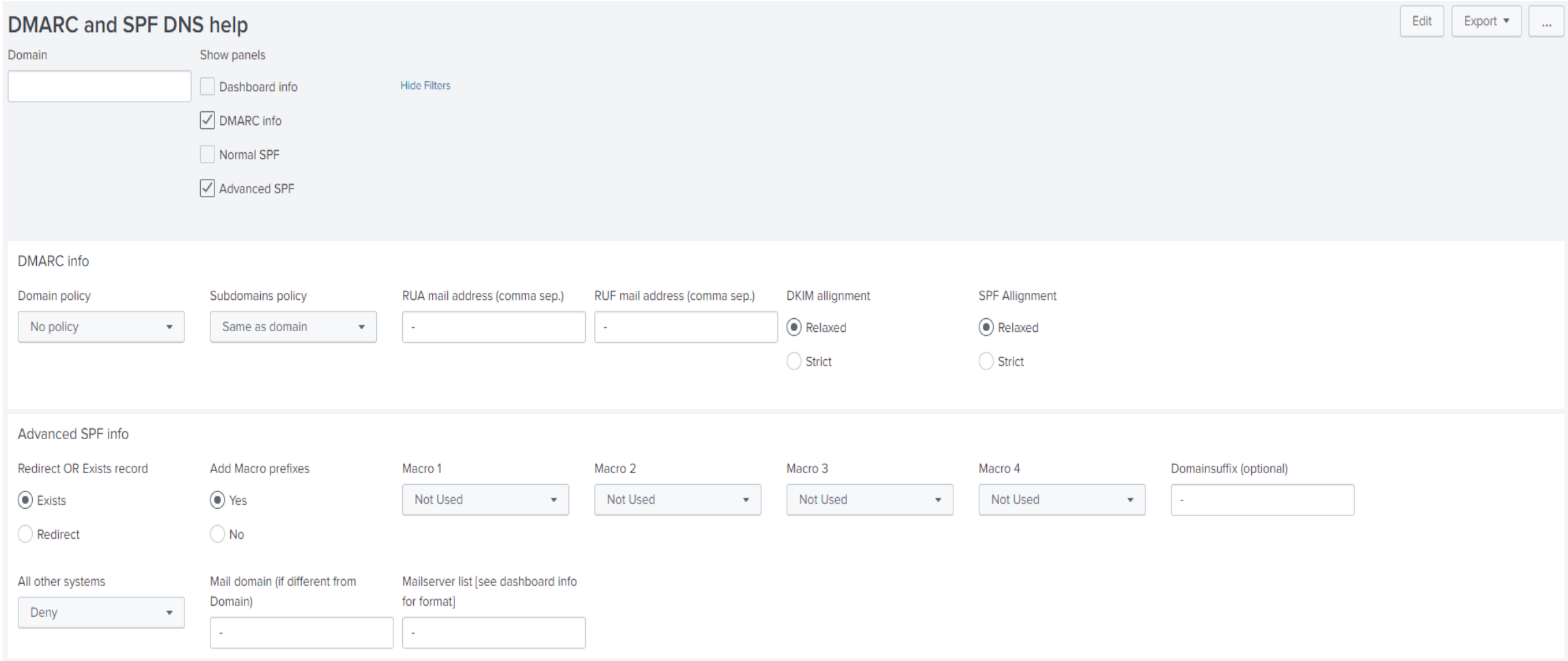
Adoption overview (W.I.P.)



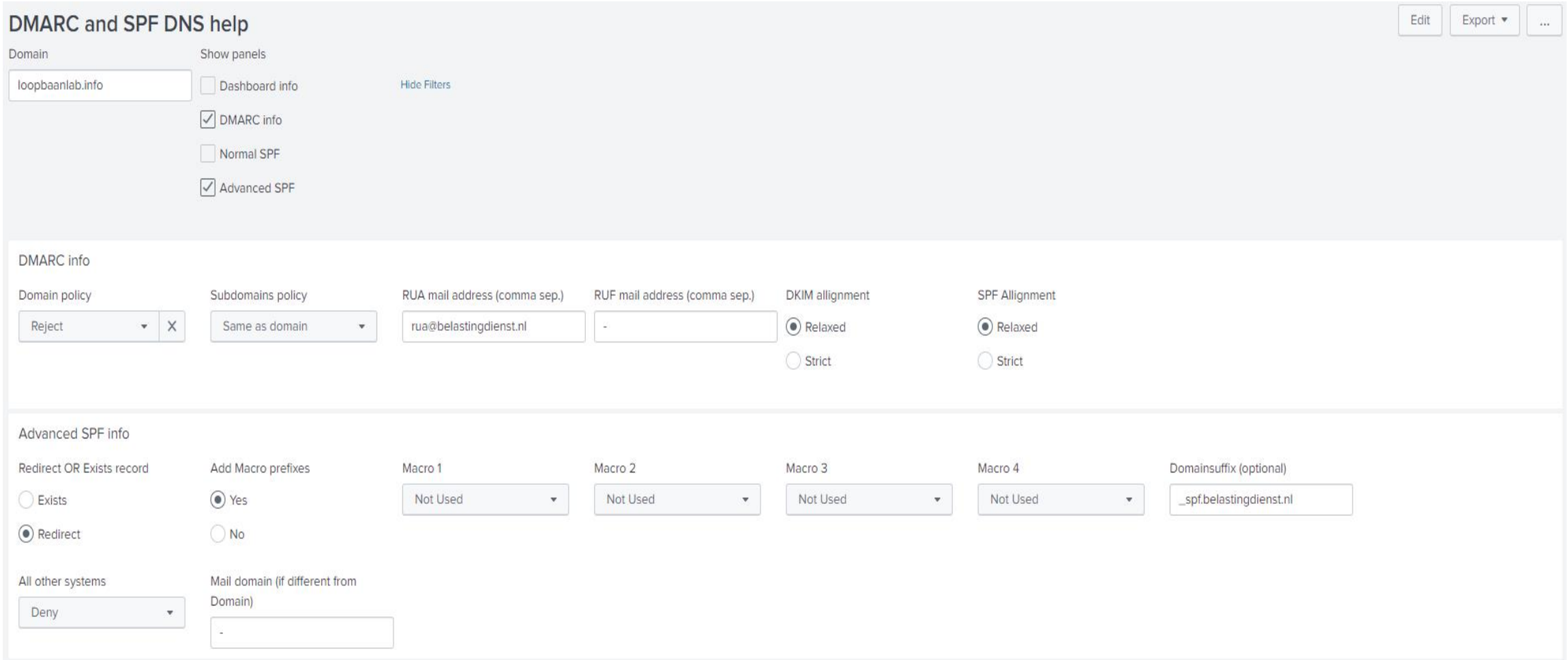
DMARC and SPF DNS help wizard



DMARC and SPF DNS help wizard



DMARC and SPF DNS help wizard



DMARC and SPF DNS help wizard

DNS records

	DNS Domain	Record Type	DNS Record	Note
1	*.loopbaanlab.info.	IN TXT	"v=spf1 -all"	Default SPF record to prevent mailing from non-existing subdomains. NOTE: you also need to create a "*" record for your subdomains. e.g.: *.acc.loopbaanlab.info
2	_dmarc.loopbaanlab.info.	IN TXT	"v=DMARC1; p=reject; rua=mailto:rua@belastingdienst.nl"	DMARC policy record
3	loopbaanlab.info.	IN TXT	"v=spf1 redirect=_spf.belastingdienst.nl"	NOTE: with an redirect record the -all must NOT be added, or the redirect record will be ignored NOTE: you also need a valid SPF record on the redirect URL
4	loopbaanlab.info._report._dmarc.belastingdienst.nl.	IN TXT	"v=DMARC1"	DMARC record to allow the cross domain sending of RUA and/OR RUF mails (rfc7489 section 7.1).

DMARC and SPF DNS help wizard

	DNS Domain	Record Type	DNS Record	Note
1	*.belastingdienst.nl.	IN TXT	"v=spf1 -all"	Default SPF record to prevent mailing from non-existing subdomains.
2	_dmarc.belastingdienst.nl.	IN TXT	"v=DMARC1; p=reject; rua=mailto:rua@belastingdienst.nl"	DMARC policy record
3	_i.85.159.100.246._h.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the RFC5321.MailFrom SPF check.
4	_i.85.159.100.246._h.smtp11.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the HELO/EHLO SPF check.
5	_i.85.159.100.4._h.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the RFC5321.MailFrom SPF check.
6	_i.85.159.100.4._h.mailer2.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the HELO/EHLO SPF check.
7	_i.85.159.101.15._h.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the RFC5321.MailFrom SPF check.
8	_i.85.159.101.15._h.smtp2.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the HELO/EHLO SPF check.
9	_i.85.159.96.4._h.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the RFC5321.MailFrom SPF check.
10	_i.85.159.96.4._h.mailer1.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the HELO/EHLO SPF check.
11	_i.85.159.97.15._h.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the RFC5321.MailFrom SPF check.
12	_i.85.159.97.15._h.smtp1.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the HELO/EHLO SPF check.
13	_i.85.159.97.246._h.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the RFC5321.MailFrom SPF check.
14	_i.85.159.97.246._h.smtp12.belastingdienst.nl._o.belastingdienst.nl._spf.belastingdienst.nl.	IN A	127.0.0.1	The exists option needs to have any A record to work. See RFC7208 section 5.7 This record is for the HELO/EHLO SPF check.

Lessons Learned

- Investigate where all your e-mail servers are located. The marketing department often use different e-mail servers for campaigns.
- Monitor your e-mail server logs.
- Test, test, test your SPF policy and DMARC policy. Must be in production!
- Don’t forget to create a SPF record for your (non) existing subdomains with a wildcard DNS resource record!
- Splunk Dashboards and code can be found on:
  https://github.com/aholzel

Final Thoughts

- Get more insight into who is sending e-mails pretending to be you and/or your organization.
- The information can be used to gain more visibility in the e-mail servers your organization is using. You will be surprised, we were!
- Implementation must be done in the production environment. And yes, it can be done, we have done it without major issues.
- A rollout can only be successful if your MTA administrators, SOC Analysts and NOC engineers and the business work closely together.
- Please only use standards defined in RFCs to avoid compatibility issues.

Resource overview

Splunk App	https://github.com/aholzel
RFC3207 (SMTP)	https://tools.ietf.org/html/rfc3207
RFC6376 (DKIM)	https://tools.ietf.org/html/rfc6376
RFC6698 (DANE-TLSA)	https://tools.ietf.org/html/rfc6689
RFC7208 (SPF)	https://tools.ietf.org/html/rfc7208
RFC7489 (DMARC)	https://tools.ietf.org/html/rfc7489
RFC7672 (DANE-TLS)	https://tools.ietf.org/html/rfc7672
RFC8460 (TLS reporting)	https://tools.ietf.org/html/rfc8460
RFC8461 (MTA-STS)	https://tools.ietf.org/html/rfc8461
SPF statistics	https://spf-all.com/stats.html
DMARC adoption report	https://250ok.com/email-deliverability/how-has-dmarc-adoption-evolved-since-2018-its-complicated/

Thank you!