Best Practices on Email Protection: SPF, DKIM and DMARC

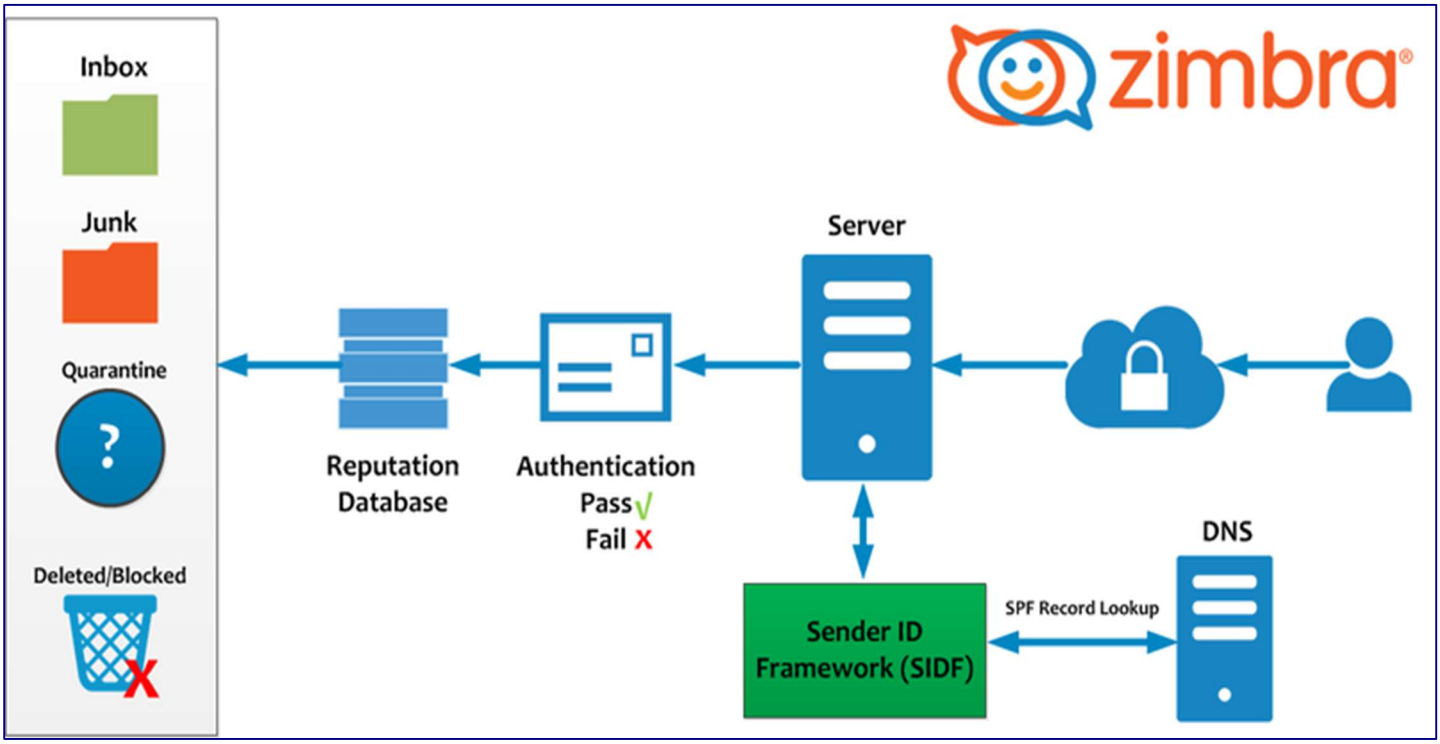
Table of Contents

Best Practices on Email Protection: SPF, DKIM and DMARC 1
SPF 1
Where needs to be configured? 2
How to configure it? 2
Understand the "all" feature in the SPF entry 3
Difference between ~all and -all 3
How to test it 3
Deprecated SPF RR, use TXT RR only 4
DKIM 4
Where needs to be configured? 5
How to configure it? 5
How to test it 5
2048-bit signatures starting ZCS 8.7.x 5
How to check that you have a valid DKIM signature 6
DMARC 7
Where needs to be configured? 8
How to configure it? 8
How to test it 9
rDNS 10
Where needs to be configured? 10
How to configure it? 10
How to test it 10
Zimbra Settings For DMARC Alignment 11
Out Of Office Replies (Auto Responders) 11
Zimbra Web Client Personas 11

Once we installed Zimbra Collaboration, we need to be aware of some additional configurations that will allow us to send emails to other Email systems with an improve Security, such Gmail, Hotmail, Yahoo!, etc. This Wiki article will show the different Email Protection resources that exists, depends of the volume of sent email, will be better to implement only one, or two, or maybe all of them, depends.

SPF

Sender Policy Framework (SPF) is an email validation system, designed to prevent unwanted emails using a spoofing system. To check this common security problem, SPF going to verify the source IP of the email and compare it with a DNS TXT record with a SPF content.



Where needs to be configured?

SPF needs to be configured in the Public DNS

How to configure it?

First of all, generate the TXT SPF DNS entry (using the MXToolbox SPF Tool, or something similar), for example with the domain called domain.com and have 3 different entries to add:

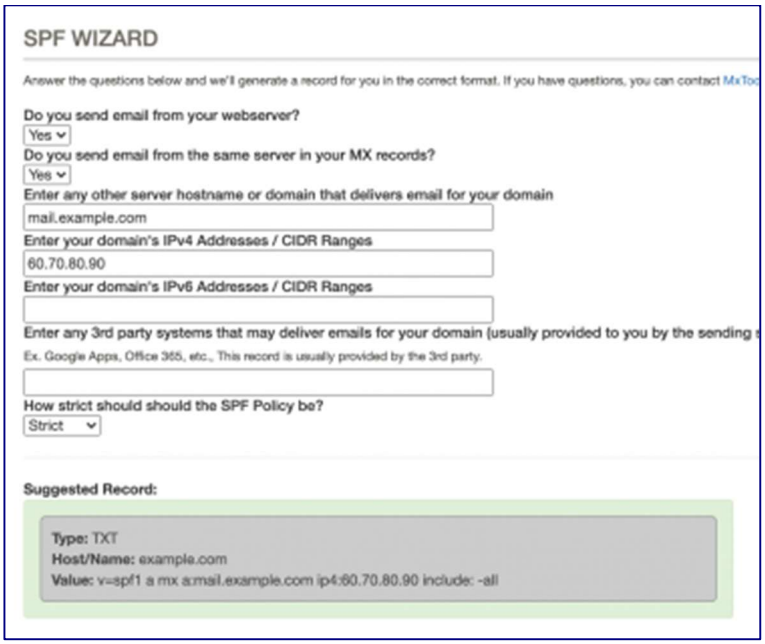
- The A entry - mail.domain.com
- The MX entry - srvmta.domain.com
- The IPv4 entry - 60.70.80.90

If in your email system you are using external services like Mailchimp, Salesforce, etc. add them in the include part, for example:

- include:servers.mcsv.net (Mailchimp)
- include:_spf.salesforce.com (Salesforce)

- include:_spf.google.com (Google Apps)

An example will look like:



Understand the "all" feature in the SPF entry

SPF can be configured in different ways, since **neutral** to **hard fail**. Almost 98% of domains are using the ~all (softfail) that means even if something of the SPF entry is wrong against the source Mailserver, mark the mail only like softfail. Here, the complete table to understand the feature **all** in the SPF

Parameter	Result	Means
+all	pass	Permits all the email, like have nothing configured.
-all	fail	Will only mark the email like pass if the source Email Server fits exactly, IP, MX, etc. with the SPF entry.
~all	softfail	Allows to send the email, and if something is wrong will mark it like softfail.
?all	neutral	Without policy

Difference between ~all and -all

If your domain is under an SPAM attack trying to spoofing your domain, try to change the SPF to -all for a while, and reset to ~all when the attack ends. Keep selected the -all if you want to be strict with the SPF entry and you are sure that your DNS entry is correct.

How to test it

Have a lot of SPF tools to check if the DNS entry is correct, for example:

- **http://tools.wordtothewise.com/spf** (will show an overview of all the allowed IPS that can send using the domain)

- **http://www.kitterman.com/spf/validate.html** (Simple but effective, will show the SPF DNs entry and also the result: pass, softfail, fail, neutral, etc.)
- **http://mxtoolbox.com/** A Classic

Deprecated SPF RR, use TXT RR only

In April 2014, the SPF DNS record was deprecated in the RFC, and the correct way to implement the SPF is using only a TXT DNS record. For example, this **was a valid DNS entries before April 2014**, TXT and SPF:

```
3.1.1.  DNS Resource Record Types

   This document defines a new DNS RR of type SPF, code 99.  The format
   of this type is identical to the TXT RR [RFC1035].  For either type,
   the character content of the record is encoded as [US-ASCII].

   It is recognized that the current practice (using a TXT record) is
   not optimal, but it is necessary because there are a number of DNS
   server and resolver implementations in common use that cannot handle
   the new RR type.  The two-record-type scheme provides a forward path
   to the better solution of using an RR type reserved for this purpose.

   An SPF-compliant domain name SHOULD have SPF records of both RR
   types.  A compliant domain name MUST have a record of at least one
   type.  If a domain has records of both types, they MUST have
   identical content.  For example, instead of publishing just one
   record as in Section 3.1 above, it is better to publish:

     example.com. IN TXT "v=spf1 +mx a:colo.example.com/28 -all"
     example.com. IN SPF "v=spf1 +mx a:colo.example.com/28 -all"
```

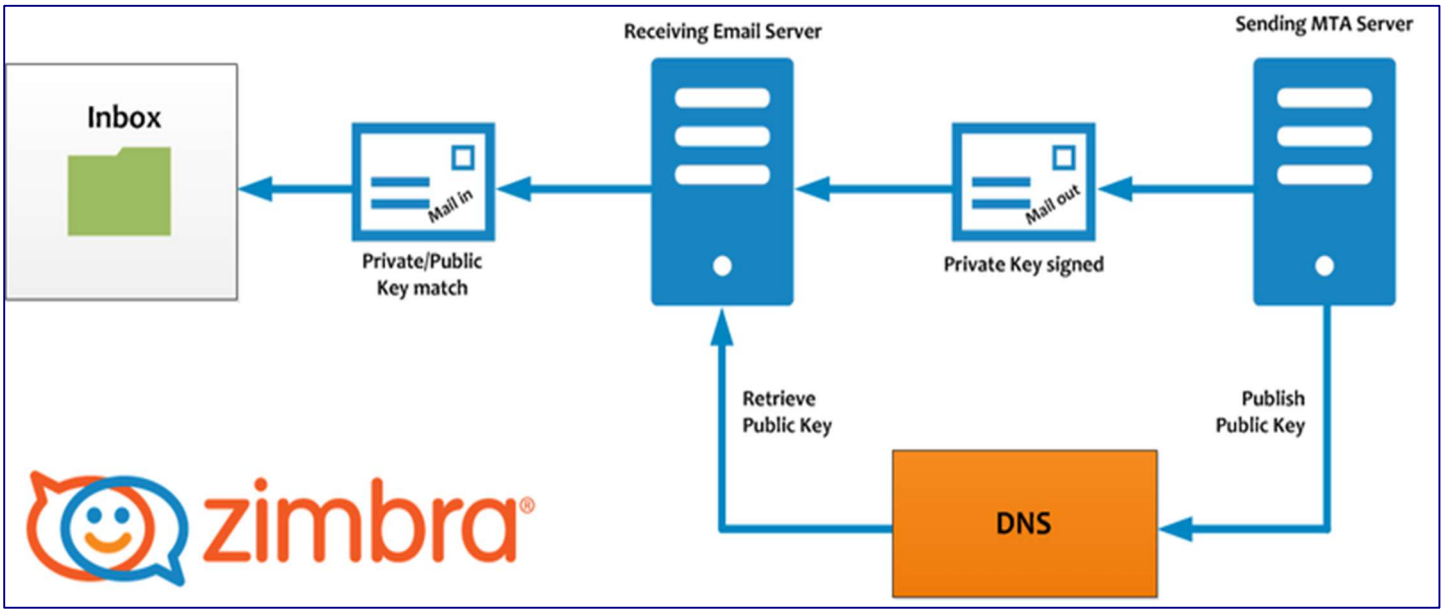
And here the RFC text where you can find the part about use only TXT:

```
3.1.  DNS Resource Records

   SPF records MUST be published as a DNS TXT (type 16) Resource Record
   (RR) [RFC1035] only.  The character content of the record is encoded
   as [US-ASCII].  Use of alternative DNS RR types was supported in
   SPF's experimental phase but has been discontinued.

   In 2003, when SPF was first being developed, the requirements for
   assignment of a new DNS RR type were considerably more stringent than
   they are now.  Additionally, support for easy deployment of new DNS
```

- **RFC before April 2014**
- **RFC after April 2014**

DKIM

DomainKeys Identified Mail (DKIM), is a method to associate the domain name and the email, allowing to a person or company assume the responsibiltity of the email.



Where needs to be configured?

DKIM needs to be generated per domain in our Zimbra Server, and needs to be configured in the public DNS of each domain.

How to configure it?

To configure properly DKIM, please follow the next Wiki - Configuring_for_DKIM_Signing

Once have the DKIM generated in Zimbra, add the info in the public DNS, will looks like:

How to test it

Have multiple websites to test it, for example:

- http://dkimvalidator.com You need to send a email, once you have the DKIM configured, then in the website will found a section called DKIM and the result in the end, if the test is passed or not.

2048-bit signatures starting ZCS 8.7.x

Starting ZCS 8.7.x Zimbra generates a 2048-bit key, after run the next command (mind the -a if it's the first time, and -u if you are updating the DKIM):

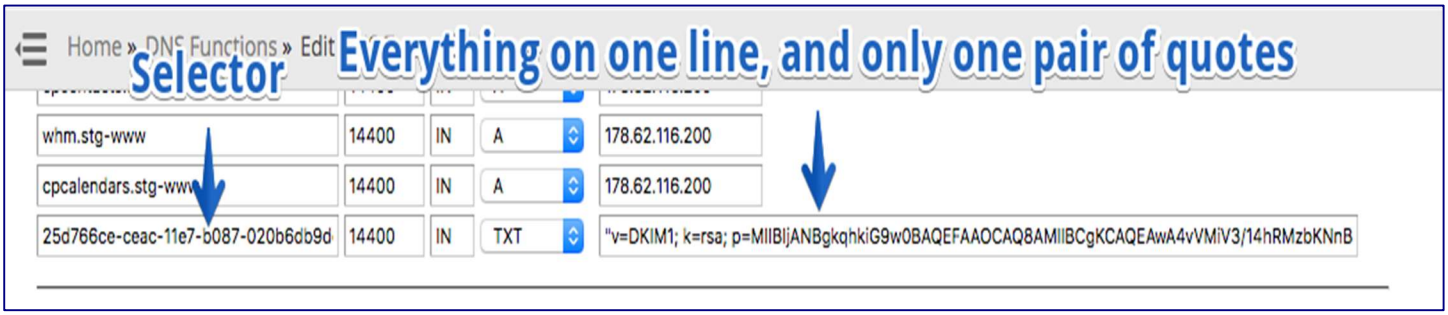
```
/opt/zimbra/libexec/zmdkimkeyutil -a -d yourdomain.com
```

You will observe something like the next (with your own information):

```
DKIM Data added to LDAP for domain zimbra.io with selector 25D766CE-CEAC-11E7-B087-
020B6DB9DD9A
Public signature to enter into DNS:
25D766CE-CEAC-11E7-B087-020B6DB9DD9A._domainkey IN      TXT     ( "v=DKIM1; k=rsa;
"

"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwA4vVMiV3/14hRMzbKNnBKNThqxTWLi2E5Nq
qHLccIJg/P33yqwgGVKKUM9HFfXZ8urz6/dl8oNG3oxs73W1sgWHrFRo3ZayHsuUMe+DLyt8wtyR/RUae0n
vd6Z6t0lPwujXWBrRS/FeMg/IGA8ExBKjD+aAYdQfH/lhlDGzumTXgbSB0KMzlpOjcum2Aes69rEiR744GG
aPb2"

"X3MxK8vjpeMIx16n2tADb0wKKP19WTF0at5HCP8F4SFflLUPJMOC1Be9FCWjTjNr1qrRZTwCwC7OC9tnV7
SsKKXG+8D6hu39Tm5U1GLzpKvLMIv14b6MWsU9cV/iVKH+hQq4YRowIDAQAB" )  ; ----- DKIM key
25D766CE-CEAC-11E7-B087-020B6DB9DD9A for zimbra.io
```

By default, DNS Servers only accepts 255 characters on every TXT entry, so depending on the DNS Server you are using you will need to do one of the next:

- On cPanel UI it's as easy at creating one new TXT entry with the selector, and on the value all together like "v=DKIM1; k=rsa; p=ALL-THE-CODE-"



- If using old version of Bind, or other DNS Server based in CLI, you can try by adding the DNS entry on the next format:

```
25D766CE-CEAC-11E7-B087-020B6DB9DD9A._domainkey    IN    TXT    ("v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w..."
25D766CE-CEAC-11E7-B087-020B6DB9DD9A._domainkey    IN    TXT    "...AQAB")
```

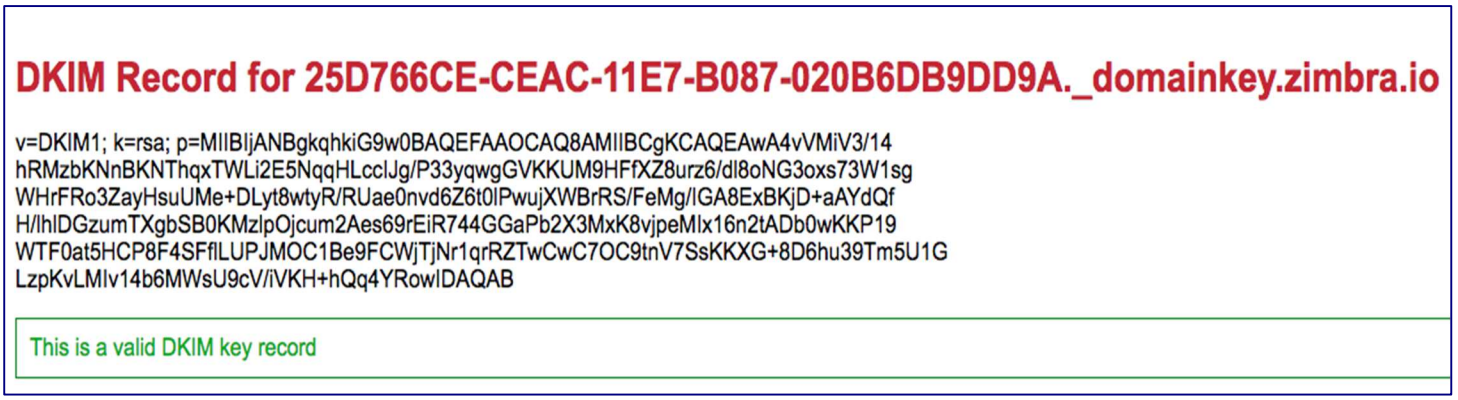
- Another way some DNS Servers might work are the next one:

```
25D766CE-CEAC-11E7-B087-020B6DB9DD9A._domainkey IN      TXT     ("v=DKIM1;k=rsa;
p="
"MIIBIjANBgkqhkiG9w..."
"...AQAB")
```

How to check that you have a valid DKIM signature

You can check if you have a valid DKIM by using for example the next URL - http://dkimcore.org/tools/keycheck.html : Introduce your selector and your domain and click on check

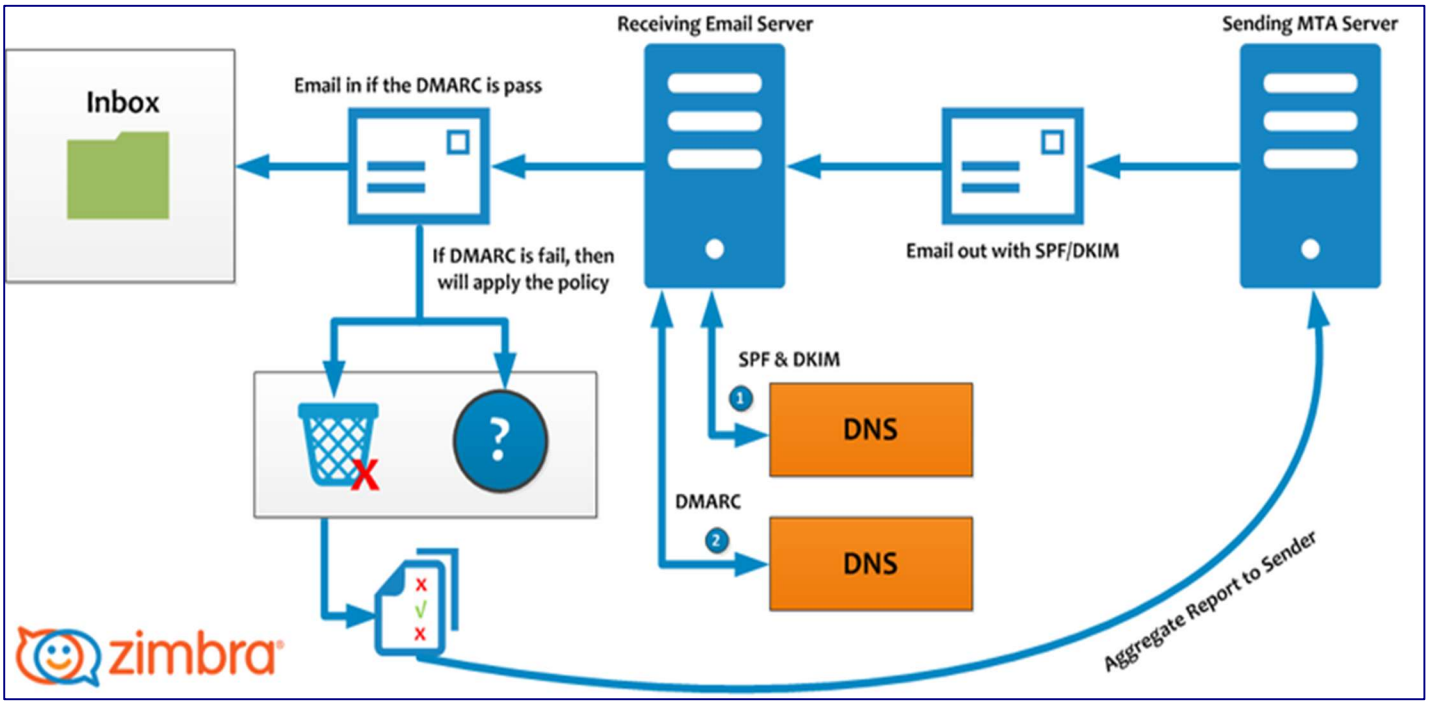
After a few seconds you will see the result:



DMARC

DMARC, which stands for “Domain-based Message Authentication, Reporting & Conformance”, is a technical specification created by a group of organizations that want to help reduce the potential for email-based abuse by solving a couple of long-standing operational, deployment, and reporting issues related to email authentication protocols.

DMARC standardizes how email receivers perform email authentication using the well-known SPF and DKIM mechanisms. This means that senders will experience consistent authentication results for their messages at AOL, Gmail, Hotmail, Yahoo! and any other email receiver implementing DMARC. We hope this will encourage senders to more broadly authenticate their outbound email which can make email a more reliable way to communicate.



Text and Image inspired from [the Official dmarc org website]

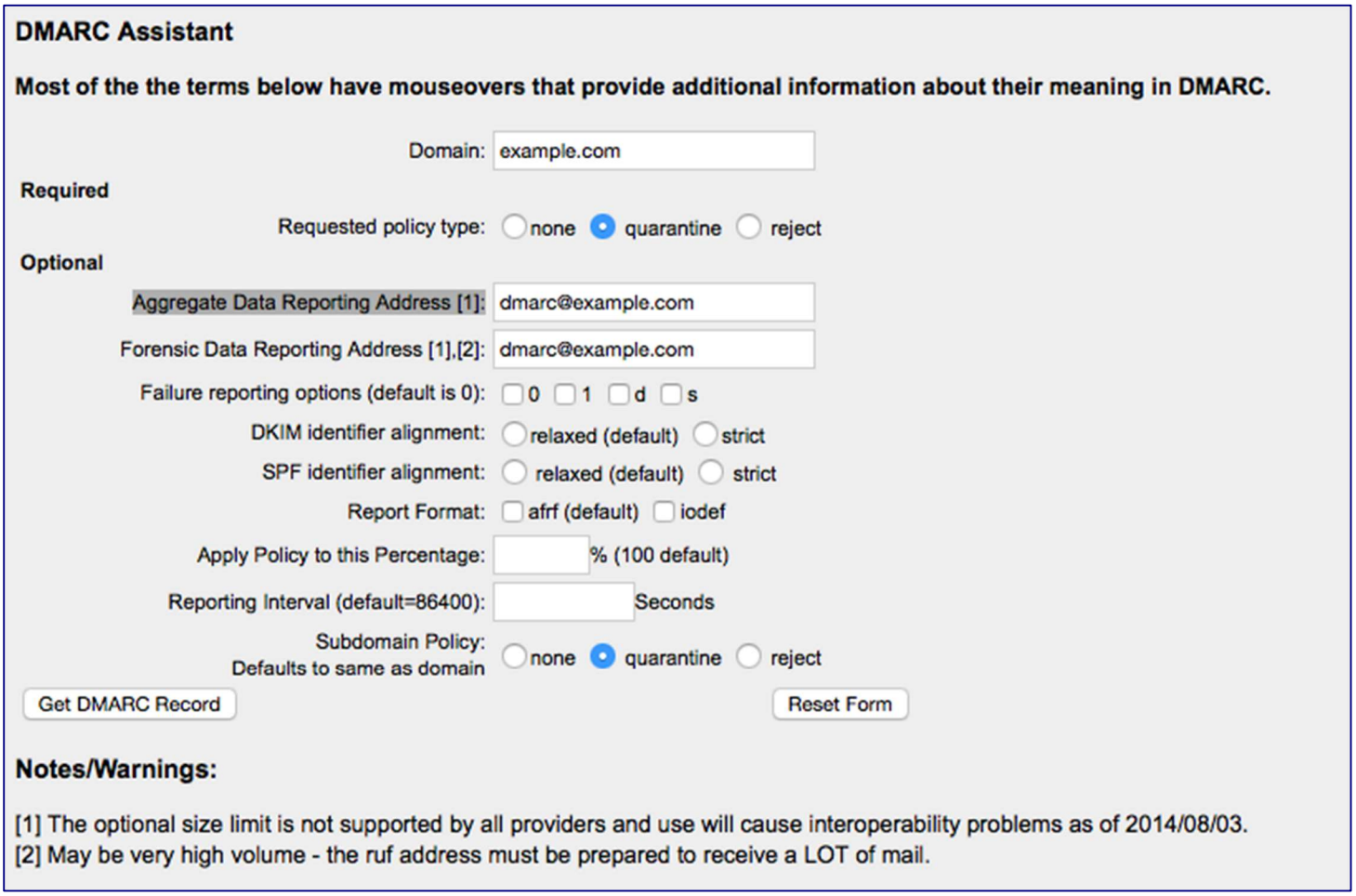
Where needs to be configured?

The DMARC needs to be configured in the public DNS.

How to configure it?

The DMARC record can be generated in multiple websites, for example
http://www.kitterman.com/dmarc/assistant.html

Using the domain example.com, a possible option can be the next, please note that all the default options will be included implicit, even if you don't select them in the generator:



This configuration will generate the next DNS entry

- DMARC record for: example.com
- Record should be published at _dmarc.example.com
- v=DMARC1; p=quarantine; rua=dmarc@example.com; ruf=dmarc@example.com; sp=quarantine

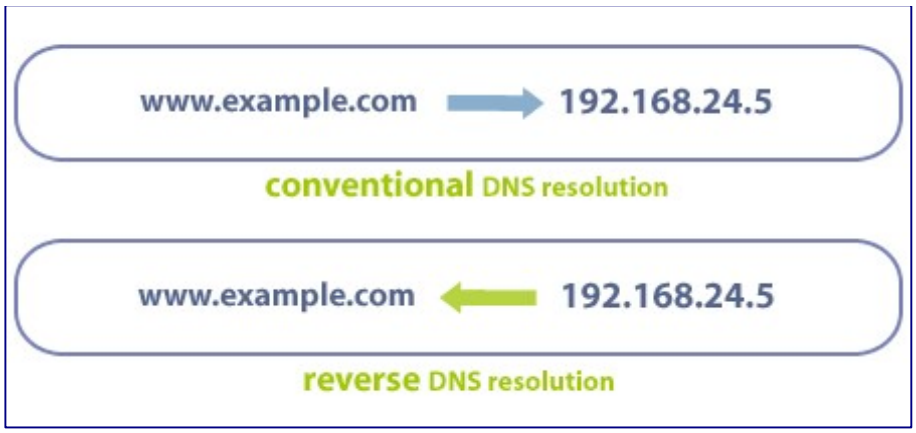
And will looks like this in a DNS with web interface:

How to test it

One of the best Sites to test the DMARC is the next link - **https://dmarcian.com/dmarc-inspector/google.com** is coming with the google.com domain per default. This website will show you all the DMARC information about your domain.

rDNS

The reverse DNS resolution (rDNS) is a determination of the domain name that is associated to an IP. Some email companies like AOL, for example, will reject any email that doesn't have a valid rDNS.



Where needs to be configured?

To have a perfect match between the rDNS and the SMTP Banner of the server, need to have the next:

- In the public DNS of the ISP provider. Or if you have control of the public DNS of your IP range, then you can add the rDNS by yourself.
- In the Zimbra Server, need to edit the HELO to match between it and the rDNS record.

How to configure it?

To modify the Public DNS to match the IP and the rDNS, you need to contact with your ISP provider, or if you have acces to edit the DNS record of your IP, then change it by yourself. For example, if you have the IP 60.60.60.60 and needs to resolve to mail.example.com.

To edit the SMTP Banner and match it with the external rDNS. Need to edit the next in Zimbra:
Zimbra 8.0.X

```
zmlocalconfig -e postfix_smtpd_banner="mail.example.com"
zmcontrol restart
```

Zimbra 8.5, 8.6, and above

```
zmprov ms  `zmhostname` zimbraMtaSmtpdBanner mail.example.com
zmcontrol restart
```

How to test it

Use the next tool - **http://mxtoolbox.com/ReverseLookup.aspx** and fill it with your Public IP, if you have everything well configured, will return the name that you want.

Zimbra Settings For DMARC Alignment

Out Of Office Replies (Auto Responders)

Check your zimbraAutoSubmittedNullReturnPath global setting to ensure it is set to false. As the Zimbra user (su - zimbra) run:

- zmprov gcf zimbraAutoSubmittedNullReturnPath
- zmprov mcf zimbraAutoSubmittedNullReturnPath FALSE

If this is set to False, it will cause the Return Path address in Out Of Office Replies to an empty value like <>

This may cause SPF alignment to fail when your DMARC policy is set to quarantine or reject. Newer Zimbra versions should default this setting to False, but older installs may be using a value of True

Zimbra Web Client Personas

If you have mailbox setup of user@domain1.com, with an alias of user@domain2.com. 2. From the Zimbra Web Client, create a Persona for user@domain2.com. 3. When a message is sent with the user@domain2.com Persona selected, the following occurs:

- The Return Path email address is set to: user@domain2.com
- The From header email address is set to: user@domain1.com
- If your DMARC policy is set to quarantine or reject, this will cause the SPF alignment test to fail.

To Change This Behavior, set the zimbraSmtpRestrictEnvelopeFrom value to False for either an individual user, a domain, or a Class Of Service. For example, to change this setting for an individual user, as the Zimbra user (su - zimbra):

- zmprov ma user@domain1.com zimbraSmtpRestrictEnvelopeFrom FALSE

Further reading : https://blog.zimbra.com/2022/04/email-security-webinar-about-dmarc/