TECHNICAL GUIDELINE

SUBJECT	SPF policy University of Twente
VERSION	1.0
DATE	01-04-2020
AUTHOR(S)	Peter Peters

INTRODUCTION

The University of Twente has measures in place to support and promote a safe email environment. Part of that environment is Sender Policy Framework (SPF). SPF consists of a nameserver entry (SPF RR) telling mailservers how to handle email from our domain. In short, SPF tells a receiving mail server which servers are allowed to send email using our addresses. It also tells the receiving server what it should do with email that does not come from the designated servers.

LIMITATIONS

SPF has some limitations[1] in its use. An SPF RR has a practical limit of 255 characters. This means we are limited to the number of entries, either host names of IP addresses, we can include. SPF offers a solution by referring to other SPF RR's. If they are in the same domain the total of both SPF RR's should not exceed roughly 460 characters. The third, and most dangerous limit is the number of requests a mail server should need to resolve the SPF RR. That number is ten (10).

While we can control the first two limitations, the latter is hardly manageable if we refer to external SPF records, like when using cloud service providers who want to send out email with our addresses. Look, for instance, at the SPF RR for student.utwente.nl:

```
v=spf1 include:_spf.google.com include:_spf.snt.utwente.nl -all
```

This simple SPF RR only has two referers but still the receiving mail server has to perform eight queries to decide whether the sending server is allowed to. Adding one or two extra referers results in a mail server not being able to do a full query and it will most probably refuse to accept the email.

If a SaaS provider wants to send out email with our addresses it always asks us to add their servers to our SPF RR.

[1] https://www.socketlabs.com/blog/best-practices-sender-policy-framework-spf/

```
v=spf1 include:_spf.example.com -all
```

That doesn't seem so bad. Except when another SaaS provider has the same request.

```
v=spf1 include:_spf.example.com include:_spf.example.nl -all
```

Because we don't know how many referers those companies use in their SPF RR we have no idea if or when the limit of ten queries is reached.

DANGER OF OVERASSIGNING

In the example of student.utwente.nl we see a referral to google.com. This is possible because Google keeps tight control on what servers are allowed to send email from the Google network and for what domains. That is different for Google cloud, or any other major IaaS provider like Amazon and Microsoft.

A SaaS provider may be using Amazon and ask us to add Amazon SES to our SPF RR.

```
v=spf1 include:_spf.amazonses.com -all
```

Because the SaaS provider does not know on what machine his software is running -it's the cloud, after all- he can't narrow it down. So by using this entry in our SPF RR suddenly all customers of Amazon SES can send email using our addresses.

Even though we trust Amazon we can't trust its customers, as is also the case with Azure or Google Cloud.

DOMAINS WITHOUT EMAIL

The email policy restricts email to only a few domains. Other domains must not be used to send or receive email. To prevent criminals using these domains to phish we should publish an SPF RR indicating that any email from these domains should be treated as phishing.

This can include domains outside of utwente.nl.

DOMAINS FOR STUDENT ASSOCIATIONS AND THIRD PARTIES

Student associations and some other third parties have their own domains, either under utwente.nl or separately. They are responsible for their own email and anti-phishing protection. The university

should help them set up correct protection. If they choose otherwise we should take measures to prevent their measures from interfering with ours.

POLICY

This results in the following policy rules for requests for SPF RR entries.

1. For utwente.nl only our official mail servers will be included in the SPF RR.
   `v=spf1 mx a:smtppool.utwente.nl include:_spfout.mf.surf.net -all`[2]
2. Sub-domains for student associations and third parties are free to use whatever SPF RR they want. We urge them to adhere to this policy as much as possible, though.
3. If a SaaS provider needs to send email using our addresses, we should urge them to make use of our SMTP server to send email. These emails will fall under the configuration of the central SPF RR.
4. If it is not possible for a SaaS provider to send email through our servers and he wants to use SPF, a separate email domain must be configured with the requested SPF RR.
   `v=spf1 include:_spf.example.com -all`
   The SaaS provider is responsible for adhering to the limits imposed on SPF RR's for this domain.
5. Emails with addresses including other subdomains, e.g. for departments, are not allowed. The same goes for other domains under responsibility of the university. An SPF RR to indicate that should be configured for each (sub)domain.
   `v=spf1 -all`
6. The university is responsible for its domains. When abuse is detected, or for any other reason, the university can change any SPF RR as it sees fit.

[2] The policy mentions -all. During the transition ~all will be used.