SPF - **DNS Resource Record**, a discussion topic

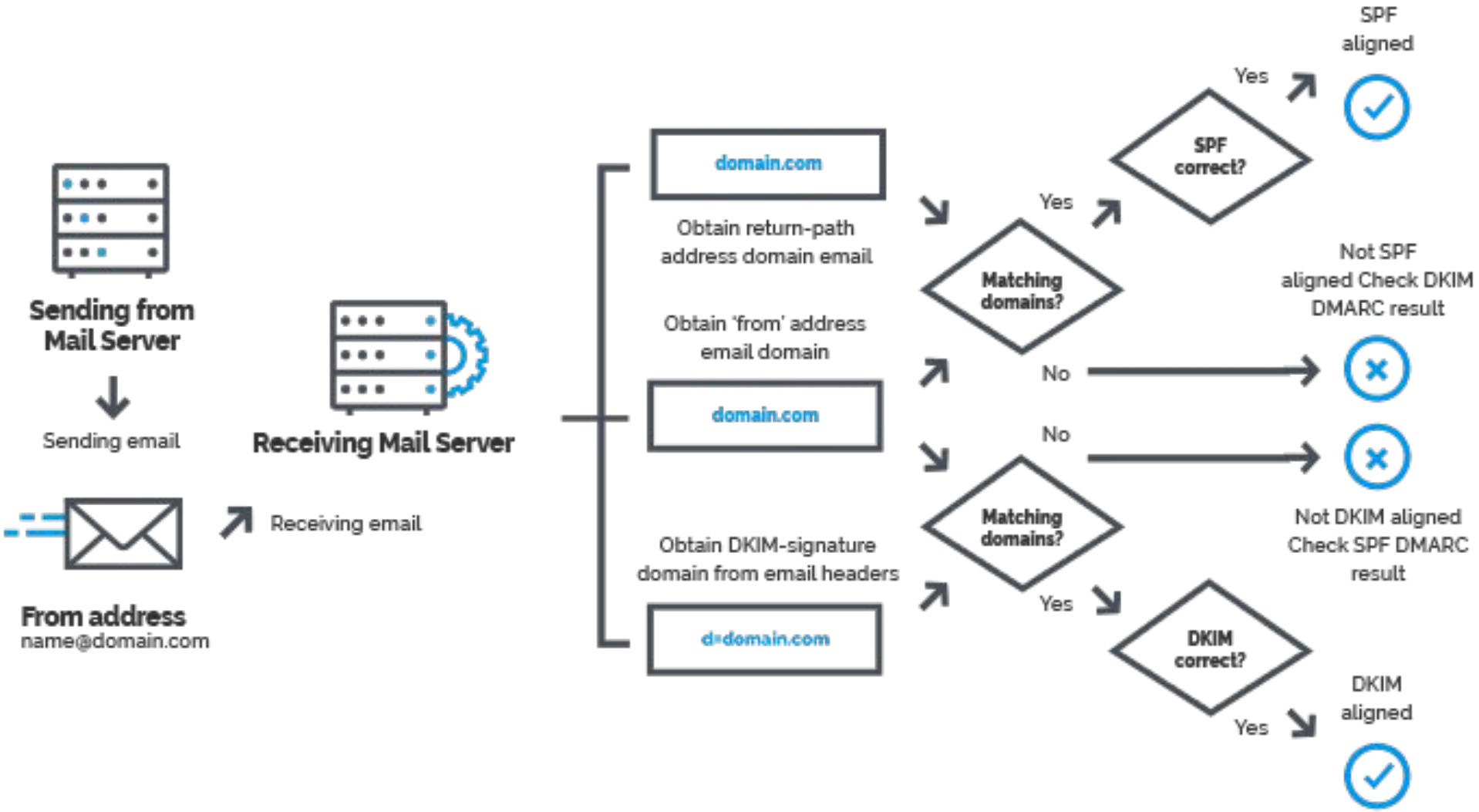
February 20, 2020

St. Louis Linux Users Group

By David Forrest

Biography

David Forrest graduated from Oregon State University in BA, Finance Emphasis, Physics & Mathematics. Lifelong hobbyist in IT from IBM 1401, Model 20, Model 30, Model 85, Sigma 7, XDS 7, SWTP 6800, M6809, 8080, 80286, 80386, OS2, and on to currently running XP, CentOS6/7, Raspbian, Mint, and Chrome on various local and cloud machines.


Sending from Mail Server
Sending email
From address
name@domain.com
Receiving email
Receiving Mail Server
domain.com
Obtain return-path address domain email
Obtain 'from' address email domain
domain.com
Obtain DKIM-signature domain from email headers
d=domain.com
Matching domains?
Yes
SPF correct?
Yes
SPF aligned
No
Not SPF aligned Check DKIM DMARC result
Matching domains?
No
Not DKIM aligned Check SPF DMARC result
Yes
DKIM correct?
Yes
DKIM aligned

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"

RFC 4408: E-mail on the Internet can be forged in a number of ways. In particular, existing protocols place no restriction on what a sending host can use as the reverse-path of a message or the domain given on the SMTP HELO/EHLO commands. This document describes version 1 of the Sender Policy Framework (SPF) protocol, whereby a domain may explicitly authorize the hosts that are allowed to use its domain name, and a receiving host may check such authorization.

SPF [RFC7208] uses two identities from the SMTP session: the host name in the EHLO command and the domain in the address in the MAIL FROM command. Since the EHLO command precedes the server response that tells whether the server supports the SMTPUTF8 extension, an IDN host name MUST be represented as A-labels. An IDN in MAIL FROM can be either U-labels or A-labels.

BUT THEN >>>>>>>>>> !!!!!

RFC 8616 EAI Authentication June 2019

All U-labels MUST be converted to A-labels before being used for an SPF validation.

Section 2.11 of [RFC6376] defines dkim-quoted-printable. Its definition is modified in messages with internationalized header fields so that non-ASCII UTF-8 characters need not be quoted. The ABNF [RFC5234] for dkim-safe-char in those messages is replaced by the following, adding non-ASCII UTF-8 characters from [RFC3629]:

```
dkim-safe-char      =  %x21-3A / %x3C / %x3E-7E /
                       UTF8-2 / UTF8-3 / UTF8-4
                    ; '!' - ':', '<', '>' - '~', non-ASCII

UTF8-2              = <Defined in Section 4 of RFC 3629>

UTF8-3              = <Defined in Section 4 of RFC 3629>

UTF8-4              = <Defined in Section 4 of RFC 3629>
```

Section 3.5 of [RFC6376] states that IDNs in the d=, i=, and s= tags of a DKIM-Signature header field MUST be encoded as A-labels. This rule is relaxed only for internationalized message header fields [RFC6532], so IDNs SHOULD be represented as U-labels. This provides improved consistency with other header fields. (A-labels remain valid to allow a transition from older software.) The set of allowable characters in the local part of an i= tag is extended in the same fashion as local parts of email addresses as described in Section 3.2 of [RFC6532]. When computing or verifying the hash in a DKIM signature as described in Section 3.7 of [RFC6376], the hash MUST use the domain name in the format it occurs in the header field