SPF

PATRICK BEN KOETTER <P@SYS4.DE>

2022-08-30

What is SPF?

- Abbreviation for Sender Policy Framework
- IETF Standard RFC 7208
- A DNS-based mechanism to identify (un)authorized hosts sending on behalf of a domain
- A sender-side email policy mechanism

How does SPF work?

1. A senderdomain uses DNS to publish it’s email sending policy
2. The policy lists legitimate DNS records and / or IP-addresses / -ranges that may send email on behalf or the senderdomain
3. All hosts listed, except for the last ones quantified with `all`, may send on behalf of the senderdomain
4. A receiver checks if the client IP-address is on the list of legitimate hosts

SPF policy examples

example.com

```
example.com.  86400  IN    TXT    "v=spf1 -all"
```

sys4.de

```
sys4.de.      3600   IN    TXT    "v=spf1 ip4:194.126.158.132
ip4:194.126.158.144 ip6:2001:1578:400:111::7 -all"
```

SPF policy examples (continued...)

switch.ch

```
switch.ch.    900    IN    TXT    "v=spf1 mx:cloud.switch.ch
exists:%{ir}.spf.switch.ch include:mail.zendesk.com
include:spf.protection.outlook.com -all"
```

What problems does SPF create?

- SPF has always been considered to be br0ken by design
- The mechanism assumes a static environment, but IT isn’t
- It breaks forwarding e.g. on mailing lists
- IP has become an unreliable reputation indicator i.e. on shared platforms

How to write a SPF-policy

- Identify all legitimate hosts
- Prefer IP-notation over DNS records if possible
- Create TXT record in APEX of (sub)domain
- Monitor success / failure reports

SPF Record Anatomy

```
"<version>    <legitimate hosts>    <treatment><all others>"
```

SPF-vocabulary

- A SPF record is a DNS TXT resource record
- Statements in the record a will be evaluated left to right
- Version
- Mechanisms
- Modifier
- Qualifier

Version

- A valid SPF record MUST contain a version statement
- The version statement MUST be the first entry in the TXT record
- The only valid version statement today is `v=spf1`

Mechanisms

MECHANISM	VALIDITY
`all`	Matches any host (catchall)
`a`	Matches a DNS A record
`mx`	Matches a DNS MX record

Mechanisms (continued...)

MECHANISM	VALIDITY
`ip4`	Matches an IPv4 address (range)
`ip6`	Matches an IPv6 address (range)
`include`	Refers to another DNS entry whose record is part of this domains policy

Modifier

MODIFIER	DESCRIPTION
`redirect`	Use another domains SPF policy
`exp`	Refer to TXT record for explanation if client is rejected

Qualifier

QUALIFIER	RESULT	DESCRIPTION
+	`PASS`	Authorize (Allow) host to send
-	`FAIL`	Host is not authorized. Reject transport.
~	`SOFTFAIL`	Host is not authorized. Treat error generously

QUALIFIER	RESULT	DESCRIPTION
?	**NEUTRAL**	Host is neither authorized nor unauthorized. Treat like **PASS**

SPF-Design

- IP vs. DNS RR
- IP-address vs. IP-range
- Keep vs. handover control

IP vs. DNS RR

- Filtering costs time and ressources
- Design SPF for speed
- How many DNS lookups to resolve a MX?
- How many DNS lookups to resolve an IP?

IP-address vs. IP-range

- SPF serves to filter unauthorized mail clients
- The smaller the network the bigger the trust
- What’s the risk assessment for `sys4.de`?
- What’s the risk assessment for `bund.de`?
- What’s the risk assessment for `switch.ch`?
- What’s the risk assessment for `swisssign.ch`?
- What’s the risk assessment for `swisscom.ch`?

Policy Optimization Ideas

Production (swisssign.ch)

```
"v=spf1 include:spf.protection.outlook.com a:mx1.swisssign.com
a:mx2.swisssign.com a:mx3.swisssign.com a:mx4.swisssign.com
mx:swisssign.com -all"
```

Increase lookup performance, remove loop

```
"v=spf1 include:spf.protection.outlook.com a:91.194.146.13
a:91.194.146.14 a:91.194.146.15 a:91.194.146.16 -all"
```

Policy Optimization Ideas (continued...)

Simplify and speed up

```
"v=spf1 include:spf.protection.outlook.com a:91.194.146.0/27 -
all"
```

Reduce risk

```
"v=spf1 include:spf.protection.outlook.com a:91.194.146.8/29 -
all"
```

Keeping vs. handing over control

Two delegation modifiers – `include` and `redirect`.

include & redirect

```
    "v=spf1 include:_spf.example.com ~all"
    "v=spf1 redirect:_spf.example.com"
```

_spf.example.com

```
    "v=spf1 ip4:192.2.0.1 ip4:192.2.0.1 -all"
```

Keeping vs. handing over control (continued...)

`include`

`include` allows to (locally) control the `all` modifier.

Use it for organizations with many subdomains and / or when introducing SPF

`redirect`

`redirect` gives it all to the (remote) SPF policy

Use it for parked / null MX (sub)domains and / or when identical policy level has been reached and has become stable

Questions?