CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

SPF INTEGRATION & IMPLEMENTATION.

dnsbelgium

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Content

DOCUMENT CONTROL AND REVIEW

Document Control	
Author	
Owner	
Date created	
Last revised by	
Last revision date	

.

VERSION CONTROL

Version	Date of approval	Approved by	Description of change

Introduction: why implement SPF?

In an era when e-mail is the backbone of digital communication, securing e-mail traffic is becoming increasingly important. Cyber criminals widely exploit vulnerabilities in e-mail protocols to carry out phishing, spoofing and other forms of e-mail fraud. One of the most effective methods to mitigate these risks is the implementation of **Sender Policy Framework (SPF)**.

SPF (Sender Policy Framework) is an e-mail authentication mechanism that allows domain owners to specify which mail servers are authorised to send e-mails on behalf of their domain. Receiving mail servers use this information to check whether an incoming e-mail is legitimate. This is done by querying the SPF record of the sender's domain, which is stored in the Domain Name System (DNS). Some of the main reasons for implementing SPF are outlined below:

1. Protection against email spoofing

Email spoofing is a technique in which attackers send emails that appear to come from a trusted sender, such as a bank or an internal company address. This is one of the most common methods used in phishing attacks. SPF helps prevent such attacks by only allowing authorised servers to send e-mails on behalf of a domain.

2. Strengthening corporate reputation

A successful spoofing attack can cause serious reputational damage to an organisation. Customers and partners who receive fraudulent emails lose trust in the brand. SPF helps maintain the reliability and integrity of corporate communications.

3. Improving email deliverability

SPF helps improve the deliverability of legitimate e-mails. Without SPF, e-mails coming from a domain may be flagged as suspicious and end up in the recipient's spam folder. With SPF, e-mails are more likely to be delivered correctly.

4. Comply with compliance and regulations

In many industries, such as finance and healthcare, there are strict requirements for data security and communication protocols. SPF can be a crucial part of a broader security policy to meet these requirements.

5. Cost savings

A successful phishing or spoofing attack can lead to significant financial losses, such as recovery costs and fines. By implementing SPF, organisations can drastically reduce the risk of such incidents and thus save costs in the long run.

6. Easy implementation and broad support

SPF is relatively easy to implement via a DNS record and is widely supported by modern e-mail servers. This makes it a cost-effective and accessible measure for organisations of all sizes.

7. Synergy with other e-mail security protocols

SPF works well with other security protocols such as DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting, and Conformance). Together, these protocols form a powerful framework to ensure the security and reliability of e-mail traffic.

8. Conclusion

By implementing SPF, an organisation lays a solid foundation for a more secure and reliable e-mail system. It is a first step towards a comprehensive approach to e-mail security that helps protect not only the organisation itself, but also its customers, partners and stakeholders.

9. How does SPF work?

9.1 SPF RECORD IN DNS

A domain owner publishes an SPF record as a **TXT record** in the domain's DNS settings. This record contains a list of authorised mail servers (e.g. IP addresses, domain names or subdomains).

9.2 SENDING AN E-MAIL

When an e-mail is sent, it contains a **"MAIL FROM" address** in the SMTP headers. This is the address controlled by SPF.

9.3 CONTROL BY THE RECEIVING MAIL SERVER

Upon receiving an e-mail, the receiving mail server checks the DNS of the sender's domain to retrieve the SPF record. It then performs the following steps:

- **Extraction of the sending IP address**: The IP address of the server that sent the e-mail is determined.
- **Comparison with SPF record**: The sending IP address is checked against the list of authorised servers in the SPF record.
- **Determine result**: The receiving server evaluates the result of the SPF check and makes a decision:
    - **Pass**: The sending IP address is in the SPF record. The e-mail is accepted.
    - **Fail**: The sending IP address is not in the SPF record. The server may mark the e-mail as spam or reject it.
    - **Softfail**: The email is not fully trusted, but not rejected. Usually marked as suspicious.
    - **Neutral**: No explicit rules in the SPF record. The e-mail is processed normally.
    - **Permerror**: The SPF record is invalid or unreadable.

10. Building SPF records

SPF records are configured as TXT records in DNS. The syntax includes several mechanisms and qualifiers:

10.1 GENERAL STRUCTURE

v=spf1 <mechanisms> <modifiers>

- v=spf1: Indicates that this is an SPF record (mandatory).
- <mechanisms>: Rules that determine which servers are authorised.
- <modifiers>: optional parameters for more advanced configuration.

10.2 COMMONLY USED MECHANISMS

- ip4:<ip-address>: Authorises a specific IPv4 address or subnet.
- ip6:<ip-address>: Authorises a specific IPv6 address or subnet.
- a: Authorises the IP address associated with the "A record" of the domain.
- mx: Authorises the domain's mail servers (MX records).
- include:<domain>: Authorises SPF records from another domain (useful for external providers such as Google Workspace or Microsoft 365).
- all: Used as a terminator, indicates what to do with all unmatched addresses (e.g. -all for blocking).

10.3 EXAMPLE SPF RECORD

An SPF record for a domain sending mail via its own server (IP: 192.0.2.1) and Google Workspace would look as follows:

```
v=spf1 ip4:192.0.2.1 include:_spf.google.com -all
```

- ip4:192.0.2.1: Allows a specific IP address.
- include:_spf.google.com: Allows emails from servers authorised by Google.
- -all: Rejects all other Emails.

11. Implementation steps

11.1 DETERMINE SENDING E-MAIL SERVERS

- Identify any servers or providers sending emails on behalf of your domain.
- Don't forget external providers such as newsletter services (Mailchimp, etc.).

11.2 CONFIGURE THE SPF RECORD

- Add a new TXT record to your domain's DNS.
- Make sure the record contains all the necessary mechanisms.

11.3 TEST THE SPF RECORD

- Use online tools such as MXToolbox, https://nl.internet.nl/ or SPF Record Checker to validate your SPF record.
- Check that the SPF record is correctly implemented and parsed by DNS servers.

11.4 MONITOR EMAIL TRAFFIC

- Check that legitimate emails are delivered properly.
- Use tools such as DMARC reporting to understand SPF failures.

12. Limitations of SPF

While SPF is effective, it has some limitations:

- **Forwarding problems**: SPF often fails in e-mail forwarding because the forwarder is not in the original SPF record.
- **DNS dependency**: Recipients need to perform DNS queries, which can fail in case of network problems.
- **MAIL FROM check only**: SPF protects only the "MAIL FROM" address and not the "From" address that users see.

13. SPF in combination with other protocols

SPF works best in combination with other e-mail security protocols:

- **DKIM**: Verifies that the content of an e-mail has not been modified in transit.
- **DMARC**: Provides a policy framework to combine SPF and DKIM and report misuse.

Disclaimer

THIS GUIDE WAS PREPARED BY THE CENTRE FOR CYBERSECURITY BELGIUM IN COLLABORATION WITH DNS BELGIUM. ALL TEXTS, LAYOUTS, DESIGNS AND ELEMENTS OF ANY KIND IN THIS GUIDE ARE PROTECTED BY COPYRIGHT. EXTRACTS FROM THIS GUIDE MAY ONLY BE PUBLISHED FOR NON-COMMERCIAL PURPOSES ON CONDITION THAT THE SOURCE IS ACKNOWLEDGED. THE CENTRE FOR CYBERSECURITY BELGIUM AND DNS BELGIUM DISCLAIM ALL LIABILITY FOR THE CONTENTS OF THIS GUIDE. The information provided : - Is of a general nature only and does not address the specific situation of an individual or legal entity. - Is not necessarily complete, accurate or up-to-date. - Does not constitute professional or legal advice. - Is not a substitute for expert advice. - Does not guarantee secure protection.