DMARC SPF Alignment (aspf)

In DMARC, the "aspf" tag stands for "Alignment Mode for SPF."

aspf specifies how **SPF** (Sender Policy Framework) authentication results should be aligned with the email's *From* domain when evaluating DMARC policy.

Here is how it works:

Setting the aspf tag: In your DMARC record, you specify the "aspf" tag followed by one of two possible values:

- ("**aspf=r**") - Relaxed: This means that SPF signatures must only partially match the email's *MAIL FROM* (or "Return-Path") domain.
- ("**aspf=s**") - Strict: This requires a strict alignment between the SPF signature's *MAIL FROM* (or "Return-Path") domain. The SPF signature must exactly match the email's *MAIL FROM* (or "Return-Path") domain.

1. **Alignment of SPF authentication results**: SPF is an email authentication protocol that verifies the sender's IP address against a list of authorized sending IP addresses published in the DNS records of the sending domain. The "aspf" tag specifies how the domain specified in the SPF authentication result (retrieved from the "Return-Path" or "MAIL FROM" address) should align with the email's From domain when DMARC policy is evaluated.
2. **Relaxed vs. Strict alignment**: Similar to **DKIM alignment**, the choice between relaxed and strict alignment affects how strict the DMARC policy enforcement is regarding SPF authentication results. Relaxed alignment allows for more flexibility by matching SPF authentication results against organizational domains (the Parent Domain) or their immediate ancestor subdomains, while strict alignment requires an exact match between the SPF-authenticated domain and the email's *From* domain.
3. **Considerations**: The alignment mode specified by the "aspf" tag can impact DMARC policy enforcement and email deliverability. Choosing the appropriate alignment mode depends on your organization's email authentication practices, SPF implementation, and requirements for DMARC policy enforcement.

By setting the "aspf" tag in your DMARC record, you can specify how SPF authentication result alignment should be evaluated when enforcing DMARC policy, helping enhance email security and protect against email spoofing and phishing attacks.

Related Topics:

- What is DMARC?
- DMARC Policy Selectors & Tags Quick Reference
- DMARC None or Ignore Policy
- DMARC Quarantine Policy
- DMARC Reject Policy
- DMARC Policy Percentages
- DMARC RUA Reporting - Aggregate Reports (rua)
- DMARC RUF Reporting - Forensic Reports (ruf)
- DMARC Subdomain Policy (sp)
- DMARC DKIM Alignment (adkim)
- What is BIMI?
- What is a VMC?
- DMARC, DKIM, SPF and BIMI Info

Don't have the time or energy to learn, setup, monitor and maintain DMARC? What if you had a team of DMARC experts to do this for you?

Let us do DMARC for you. Check out Managed DMARC Services by GlowHost.