DMARCsimple – SPF Flattening Guide

DMARCsimple – SPF Flattening Guide

What is SPF and why does it break?

Sender Policy Framework (SPF) is a DNS-based mechanism that lists which servers are allowed to send mail on behalf of your domain. In complex environments, SPF records often hit DNS lookup limits and begin to fail in subtle ways.

The SPF 10 DNS lookup limit

The SPF specification recommends a hard limit of 10 DNS lookups during evaluation. Each include, a, mx, ptr or exists mechanism can contribute to this count. When the limit is exceeded, evaluators may treat the record as a permanent error (PermError), which can cause DMARC failures and deliverability problems.

What is SPF flattening?

SPF flattening is the process of resolving indirect mechanisms—especially include statements—into a direct list of IP addresses and networks. The goal is to reduce DNS lookups while preserving the set of systems that are authorized to send mail for your domain.

How SPF flattening helps DMARC

Because DMARC relies on SPF and DKIM results, a fragile SPF record can produce noisy DMARC data. Flattening reduces PermErrors, makes SPF behavior more predictable and leads to clearer, more reliable DMARC reports.

Where DMARCsimple fits today

DMARCsimple helps identify SPF issues by analyzing DMARC aggregate reports and highlighting domains at risk of exceeding lookup limits, providers that frequently fail SPF and legacy include entries that may be removed or simplified.

Best practices

• Flatten only where necessary, starting with domains at or near lookup limits.

• Review provider documentation regularly, as IP ranges can change over time.

• Document why each IP range or network is present in your SPF record.

• Pair SPF flattening with DMARC monitoring to catch unintended side effects quickly.